

Our Ref.:
KOY-5

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

----- -x
In re Application of: :
T. Takeyama :
Serial No.: : 600 Third Avenue
New York, NY 10016
Filed: Concurrently herewith :
For: MEDICAL INFORMATION :
MANAGEMENT SYSTEM :
----- -x

September 8, 2003

Commissioner of Patents
P.O. BOX 1450
Alexandria VA 222313-1450

S i r :

With respect to the above-captioned application,
Applicant(s) claim the priority of the attached application(s) as
Provided by 35 U.S.C. 119.

Respectfully submitted,

Donald C. Lucas
MUSERLIAN, LUCAS AND MERCANTI
Attorneys for Applicants
600 Third Avenue
New York, NY 10016
(212) 661-8000

Enclosed: Certified Priority Document, Japanese Patent
Application No. 2002-268710 filed September 13, 2002.

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2002年 9月13日

出願番号

Application Number:

特願2002-268710

[ST.10/C]:

[JP2002-268710]

出願人

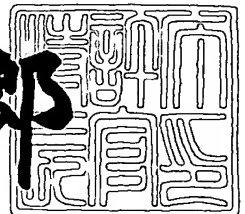
Applicant(s):

コニカ株式会社

2003年 6月10日

特許庁長官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3045330

【書類名】 特許願
【整理番号】 DKY00767
【提出日】 平成14年 9月13日
【あて先】 特許庁長官 殿
【国際特許分類】 G06F 13/00
G06F 7/00
G06F 9/00 310

【発明者】

【住所又は居所】 東京都日野市さくら町1番地 コニカ株式会社内
【氏名】 竹山 敏久

【特許出願人】

【識別番号】 000001270
【氏名又は名称】 コニカ株式会社

【代理人】

【識別番号】 100090033
【弁理士】
【氏名又は名称】 荒船 博司

【手数料の表示】

【予納台帳番号】 027188
【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 医療情報管理システム

【特許請求の範囲】

【請求項 1】

データベースに医療情報を記憶する複数のデータベース装置と、統合的に医療情報を管理する管理装置と、前記データベース装置及び前記管理装置のうち少なくとも一方を操作する操作端末と、を備える医療情報管理システムにおいて、

データベース装置は、データベースに記憶された医療情報の中から必要な情報を抽出して前記管理装置に送信する自動送信手段を備え、

管理装置は、

前記自動送信手段から送信された医療情報を受信する受信手段と、

前記受信手段により受信された医療情報を、当該医療情報に含まれる所定の情報に基づいて統合的に記憶する記憶手段と、

前記操作端末の操作者が予め登録された個人であるか否かを照合して認証する個人照合手段と、

前記操作端末により操作指示された医療情報が操作可能な情報であるか否かを判別するデータアクセス権確認手段と、

を備えることを特徴とする医療情報管理システム。

【請求項 2】

前記管理装置は、前記個人照合手段により認証された操作者からの操作指示に基づいて、前記データアクセス権確認手段により前記操作指示された医療情報が操作可能な情報であると判別された場合に、当該医療情報の閲覧、追加、修正及び加工のうち少なくとも 1 種の操作を行わせる制御手段を備えることを特徴とする請求項 1 記載の医療情報管理システム。

【請求項 3】

医療情報を記録媒体に電子情報として記録又は印刷媒体にハードコピーとして出力する出力装置を備え、

前記管理装置は、前記操作端末により出力指示された医療情報が前記出力装置に出力可能な情報であるか否かを判別し、当該医療情報が出力可能な情報である

場合に、前記出力装置に医療情報を出力する出力許可手段を備えることを特徴とする請求項 1 又は 2 に記載の医療情報管理システム。

【請求項 4】

前記管理装置は、前記制御手段により、前記記憶手段に記憶された医療情報に追加、修正又は加工の操作が行われた場合に、変更履歴を当該医療情報に対応付けて記憶手段に記憶させるデータ改竄防止手段を備えることを特徴とする請求項 2 項に記載の医療情報管理システム。

【請求項 5】

前記管理装置は、前記制御手段により、前記記憶手段に記憶された医療情報に閲覧、追加、修正又は加工の操作が行われた場合に、当該医療情報が操作された日時を付帯情報として医療情報に付与する日時付与手段を備えることを特徴とする請求項 2 又は 4 記載の医療情報管理システム。

【請求項 6】

前記日時付与手段は、前記自動送信手段により送信された医療情報が前記受信手段により受信された日時又は前記記憶手段に記憶された日時を付帯情報として当該医療情報に付与することを特徴とする請求項 5 記載の医療情報管理システム。

【請求項 7】

前記自動送信手段は、送信する医療情報と、過去に送信した医療情報との差分を検出し、前記差分に対応する医療情報を抽出し、当該抽出された医療情報を必要な情報として管理装置に送信することを特徴とする請求項 1 記載の医療情報管理システム。

【請求項 8】

前記自動送信手段により送信される医療情報は、当該医療情報が作成された作成日時を付帯情報として含み、

前記管理装置は、受信手段により受信した医療情報に含まれる作成日時と、記憶手段に記憶されている医療情報に含まれる作成日時とを比較して、受信手段により受信した医療情報のうち作成日時の異なる医療情報を記憶手段に記憶させる記憶制御手段を備えることを特徴とする請求項 1 記載の医療情報管理システム。

【請求項 9】

前記個人照合手段は、パスワード、IDカード、指紋、掌紋、声紋、顔、署名筆跡、虹彩パターン、眼底パターンあるいは静脈パターンに基づいて個人を照合する手段の中から選ばれる少なくとも1種の個人照合手段であることを特徴とする請求項1から4のいずれか一項に記載の医療情報管理システム。

【請求項 10】

前記個人照合手段は、パスワード又はIDカードを照合させる手段と、指紋、声紋あるいは虹彩パターンを照合させる手段の中から選ばれる少なくとも1種とを組み合わせた個人照合手段であることを特徴とする請求項9記載の医療情報管理システム。

【請求項 11】

前記制御手段により、閲覧、追加、修正又は加工される医療情報は、文字データ、オンオフデータ、静止画像データ、動画データの中から選ばれる少なくとも1種のデータであることを特徴とする請求項2記載の医療情報管理システム。

【請求項 12】

前記操作端末は、操作指示を入力するための入力手段を備え、
前記入力手段は、ペン入力、キーボード入力、マウス入力あるいは音声入力から選ばれる少なくとも1種の入力手段であることを特徴とする請求項1記載の医療情報管理システム。

【請求項 13】

前記医療情報は、臨床検査管理システムデータ、放射線科情報システムデータ、病院情報システムデータ、電子カルテシステムデータ、症例管理システムデータ、薬歴管理システムデータ、医薬品文書データ、介護保険システムデータ、医療関連文献データから選ばれる少なくとも1種のデータを含むことを特徴とする請求項1から8又は11のいずれか一項に記載の医療情報管理システム。

【請求項 14】

前記自動送信手段により送信される医療情報は、臨床検査管理システムデータ、放射線科情報システムデータ、病院情報システムデータ、電子カルテシステムデータ、症例管理システムデータ、薬歴管理システムデータ、医薬品文書データ

、介護保険システムデータ、医療関連文献データから選ばれる少なくとも1種のデータを含むことを特徴とする請求項1から8、11又は13のいずれか一項に記載の医療情報管理システム。

【請求項15】

前記管理装置と前記操作端末は、ネットワークを介して接続され、当該ネットワークは、前記管理装置と前記操作端末とを接続するための専用回線により構築されていることを特徴とする請求項1記載の医療情報管理システム。

【請求項16】

前記管理装置は、

前記操作端末に送信する情報を暗号化して送信する暗号化送信手段と、

前記操作端末から送信された情報を受信して復号化する復号化受信手段と、

前記操作端末は、

前記管理装置に送信する情報を暗号化して送信する暗号化送信手段と、

前記管理装置から送信された情報を受信して復号化する復号化受信手段と、

を備えることを特徴とする請求項1又は15に記載の医療情報管理システム。

【請求項17】

前記管理手段の記憶手段は、医療情報の種類に応じて情報を記憶する複数のデータベースから構成され、

前記制御手段は、操作端末からの操作指示に応じて前記複数のデータベースから対応する医療情報を読み出して、閲覧、追加、修正及び加工のうち少なくとも1つの操作を制御することを特徴とする請求項2記載の医療情報管理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、医療情報管理システムに関する。

【0002】

【従来の技術】

近年、医療の効率化が求められている中で、院内外のネットワーク化、システム化が進んでおり、病院情報システム（HIS）、放射線科情報システム（RI

S)、画像保存転送システム(PACS)、電子カルテ、遠隔医療などを有機的に連携させるトータルシステムとしてのニーズも大きくなってきている。さらに、地域医療を効率的に行うために医療機関間でのデータの共有化も徐々に進行してきており、これにより患者の重複した検査や治療、薬の投与などが避けられるようになってきた。

【0003】

ところで、種々のデータをネットワークで接続されるようになってくると、患者の個人情報の漏洩に対するセキュリティの問題、また、種々のデータがデジタルデータとして保管されているために、データの人為的な改ざん防止の問題などについても課題となる場合がある。

【0004】

電子商取引などで採用しているデジタル署名や電子署名など、日本では「電子署名及び認証業務に関する法律」、米国では「グローバルな商取引と国内商取引における電子署名法」、欧州では「電子署名のための共同体の枠組みに関する指令」等の法律あるいは指令として出され、個人を特定することに関する取り組みが成されている。また、インターネット上では、例えばWeb標準化団体、World Wide Web Consortium(W3C)からXMLベースの電子署名技術の推奨規格などが提案されている。

【0005】

医療分野においても、例えば、患者に対して指紋照合による確認手段(例えば、特許文献1, 2参照)や、医療機関への来訪者、医療機関に出入する医療機関関係者又は医療機関内で出生した新生児に対して虹彩照合による確認手段(例えば、特許文献3, 4参照)や、患者に対して声紋照合による確認手段(例えば、特許文献5, 6参照)を導入することが提案されている。さらに、上述した各データへのアクセス可能な医療スタッフを予め制限するような試みがなされている(例えば、特許文献7~9参照)。

【0006】

【特許文献1】

特開2000-155782号公報

【特許文献 2】

特開 2 0 0 1 - 3 1 2 5 6 6 号公報

【特許文献 3】

特開 2 0 0 0 - 2 4 2 7 8 8 号公報

【特許文献 4】

特開 2 0 0 1 - 7 6 0 7 2 号公報

【特許文献 5】

特開平 8 - 7 1 1 4 8 号公報

【特許文献 6】

読会平 1 0 - 2 0 1 8 2 7 号公報

【特許文献 7】

特開 2 0 0 2 - 4 1 6 5 6 号公報

【特許文献 8】

特開 2 0 0 2 - 8 2 8 3 9 号公報

【特許文献 9】

特開 2 0 0 2 - 1 8 3 3 1 9 号公報

【0 0 0 7】

【発明が解決しようとする課題】

しかしながら、近年の医療情報のネットワーク化やインターネットによる広域利用が行われた場合、医療事故の問題、さらにはデータに記載されている情報が個人のプライバシーに関わるといった問題等が生じるため、種々の観点からセキュリティに関する要望がより高くなってきている。

【0 0 0 8】

本発明は、上記の課題を鑑みてなされたものであり、本発明の目的は、種々の医療情報が記憶されるデータベースに対するセキュリティを考慮した医療情報管理システムを提供することにある、さらに詳しくは個人照合手段により識別された個人情報に基づいて提供される医療情報を管理する医療情報管理システムを提供することである。

【0 0 0 9】

【課題を解決するための手段】

本発明の目的は、以下の構成により達成された。

【0010】

上記課題を解決するために、請求項1記載の発明は、

データベースに医療情報を記憶する複数のデータベース装置と、統合的に医療情報を管理する管理装置と、前記データベース装置及び前記管理装置のうち少なくとも一方を操作する操作端末と、を備える医療情報管理システムにおいて、

データベース装置は、データベースに記憶された医療情報の中から必要な情報を抽出して前記管理装置に送信する自動送信手段を備え、

管理装置は、

前記自動送信手段から送信された医療情報を受信する受信手段と、

前記受信手段により受信された医療情報を、当該医療情報に含まれる所定の情報に基づいて統合的に記憶する記憶手段と、

前記操作端末の操作者が予め登録された個人であるか否かを照合して認証する個人照合手段と、

前記操作端末により操作指示された医療情報が操作可能な情報であるか否かを判別するデータアクセス権確認手段と、

を備えることを特徴としている。

【0011】

請求項2記載の発明は、請求項1記載の医療情報管理システムにおいて、

前記管理装置は、前記個人照合手段により認証された操作者からの操作指示に基づいて、前記データアクセス権確認手段により前記操作指示された医療情報が操作可能な情報であると判別された場合に、当該医療情報の閲覧、追加、修正及び加工のうち少なくとも1種の操作を行わせる制御手段を備えることを特徴としている。

【0012】

請求項3記載の発明は、請求項1又は2に記載の医療情報管理システムにおいて、

医療情報を記録媒体に電子情報として記録又は印刷媒体にハードコピーとして

出力する出力装置を備え、

前記管理装置は、前記操作端末により出力指示された医療情報が前記出力装置に出力可能な情報であるか否かを判別し、当該医療情報が出力可能な情報である場合に、前記出力装置に医療情報を出力する出力許可手段を備えることを特徴としている。

【0013】

請求項4記載の発明は、請求項2記載の医療情報管理システムにおいて、

前記管理装置は、前記制御手段により、前記記憶手段に記憶された医療情報に追加、修正又は加工の操作が行われた場合に、変更履歴を当該医療情報に対応付けて記憶手段に記憶させるデータ改竄防止手段を備えることを特徴としている。

【0014】

請求項5記載の発明は、請求項1から4のいずれか一項に記載の医療情報管理システムにおいて、

前記管理装置は、前記制御手段の操作制御により、前記記憶手段に記憶された医療情報に閲覧、追加、修正又は加工の操作が行われた場合に、当該医療情報が操作された日時を付帯情報として医療情報に付与する日時付与手段を備えることを特徴としている。

【0015】

請求項6記載の発明は、請求項5記載の医療情報管理システムにおいて、

前記日時付与手段は、前記自動送信手段により送信された医療情報が、前記受信手段により受信された日時又は前記記憶手段に記憶された日時を付帯情報として当該医療情報に付与することを特徴としている。

【0016】

請求項7記載の発明は、請求項1記載の医療情報管理システムにおいて、

前記自動送信手段は、送信する医療情報と、過去に送信した医療情報との差分を検出し、前記差分に対応する医療情報を抽出し、当該抽出された医療情報を必要な情報として管理装置に送信することを特徴としている。

【0017】

請求項8記載の発明は、請求項1記載の医療情報管理システムにおいて、

前記自動送信手段により送信される医療情報は、当該医療情報が作成された作成日時を付帯情報として含み、

前記管理装置は、受信手段により受信した医療情報に含まれる作成日時と、記憶手段に記憶されている医療情報に含まれる作成日時とを比較して、受信手段により受信した医療情報のうち作成日時の異なる医療情報を記憶手段に記憶させる記憶制御手段を備えることを特徴としている。

【 0 0 1 8 】

請求項 9 記載の発明は、請求項 1 から 4 のいずれか一項に記載の医療情報管理システムにおいて、

前記個人照合手段は、パスワード、IDカード、指紋、掌紋、声紋、顔、署名筆跡、虹彩パターン、眼底パターンあるいは静脈パターンに基づいて個人を照合させる手段の中から選ばれる少なくとも 1 種の個人照合手段であることを特徴としている。

【 0 0 1 9 】

請求項 1 0 記載の発明は、請求項 9 記載の医療情報管理システムにおいて、

前記個人照合手段は、パスワード又は IDカードを照合させる手段と、指紋、声紋あるいは虹彩パターンを照合させる手段の中から選ばれる少なくとも 1 種とを組み合わせた個人照合手段であることを特徴としている。

【 0 0 2 0 】

請求項 1 1 記載の発明は、請求項 2 記載の医療情報管理システムにおいて、

前記制御手段により、閲覧、追加、修正又は加工される医療情報は、文字データ、オンオフデータ、静止画像データ、動画データの中から選ばれる少なくとも 1 種のデータであることを特徴としている。

【 0 0 2 1 】

請求項 1 2 記載の発明は、請求項 1 記載の医療情報管理システムにおいて、

前記操作端末は、操作指示を入力するための入力手段を備え、

前記入力手段は、ペン入力、キーボード入力、マウス入力あるいは音声入力から選ばれる少なくとも 1 種の入力手段であることを特徴とする。

【 0 0 2 2 】

請求項 1 3 記載の発明は、請求項 1 から 8 又は 1 1 のいずれか一項に記載の医療情報管理システムにおいて、

前記医療情報は、臨床検査管理システムデータ、放射線科情報システムデータ、病院情報システムデータ、電子カルテシステムデータ、症例管理システムデータ、薬歴管理システムデータ、医薬品文書データ、介護保険システムデータ、医療関連文献データから選ばれる少なくとも 1 種のデータを含むことを特徴としている。

【 0 0 2 3 】

請求項 1 4 記載の発明は、請求項 1 から 8、1 1 又は 1 3 のいずれか一項に記載の医療情報管理システムにおいて、

前記自動送信手段により送信される医療情報は、臨床検査管理システムデータ、放射線科情報システムデータ、病院情報システムデータ、電子カルテシステムデータ、症例管理システムデータ、薬歴管理システムデータ、医薬品文書データ、介護保険システムデータ、医療関連文献データから選ばれる少なくとも 1 種のデータを含むことを特徴としている。

【 0 0 2 4 】

請求項 1 5 記載の発明は、請求項 1 記載の医療情報管理システムにおいて、

前記管理装置と前記操作端末は、ネットワークを介して接続され、当該ネットワークは、前記管理装置と前記操作端末とを接続するための専用回線により構築されていることを特徴としている。

【 0 0 2 5 】

請求項 1 6 記載の発明は、請求項 1 又は 1 5 に記載の医療情報管理システムにおいて、

前記管理装置は、

前記操作端末に送信する情報を暗号化して送信する暗号化送信手段と、

前記操作端末から送信された情報を受信して復号化する復号化受信手段と、

前記操作端末は、

前記管理装置に送信する情報を暗号化して送信する暗号化送信手段と、

前記管理装置から送信された情報を受信して復号化する復号化受信手段と、

を備えることを特徴としている。

【 0 0 2 6 】

請求項 1 7 記載の発明は、請求項 2 記載の医療情報管理システムにおいて、
前記管理手段の記憶手段は、医療情報の種類に応じて情報を記憶する複数のデータベースから構成され、

前記制御手段は、操作端末からの操作指示に応じて前記複数のデータベースから医療情報を読み出して、閲覧、追加、修正及び加工のうち少なくとも 1 つの操作を制御することを特徴としている。

【 0 0 2 7 】

【発明の実施形態】

以下、図 1 ～ 1 9 を参照して本発明の実施の形態を詳細に説明する。ただし、発明の範囲は、図示例に限定されない。

【 0 0 2 8 】

ここで、本発明における医療情報管理システムと、本第 1 から第 7 の実施の形態における医療情報管理システム 1 0 0 とにおける各構成要素の対応関係を明示する。すなわち、本発明における管理装置は、本実施の形態の医療情報統括管理サーバ 1 a ～ 1 g に対応し、本発明のデータベース装置は、本実施の形態の医療情報データベース 2 ～ 8 に対応している。本発明の操作端末は、本実施の形態の操作端末 A ～ E、操作端末 2 0 ～ 8 0 に対応し、本発明の出力装置は、本実施の形態の出力装置 x ～ z に対応している。

【 0 0 2 9 】

また、本発明の管理装置と、本実施の形態の医療情報統括管理サーバ 1 a ～ 1 g の各構成要素の対応関係を明示すると、本発明の受信手段は、本実施の形態の受信手段 1 5 に対応し、本発明の記憶手段は、本実施の形態のデータベース 1 6 に対応する。また、本発明の個人照合手段は、本実施の形態の個人照合手段 1 2 に対応し、本発明のデータアクセス権確認手段は、本実施の形態のデータアクセス権確認手段 1 3 に対応している。また、本発明の制御手段、記録制御手段は、本実施の形態の制御部 1 1 に対応し、本発明の出力許可手段は、本実施の形態の出力許可手段 1 4 に対応している。さらに、本発明のデータ改竄防止手段は、本

実施の形態のデータ改竄防止手段 1 7 に対応し、本発明の日時付与手段は、本実施の形態の日付日時付与手段 1 8 に対応している。また、本発明のデータベース装置の自動送信手段は、本実施の形態の医療情報データベース 2 ～ 6 の自動送信手段 2 1 ～ 6 1 に対応している。

【 0 0 3 0 】

まず、本実施の形態の構成を説明する。

図 1 は、例えば一つの医療機関内において、医療情報統括管理サーバ 1 により医療情報を一元管理する医療情報管理システム 1 0 0 のシステム構成を示す概念図である。図 1 に示すように、医療情報統括管理サーバ（以下、「管理サーバ」と省略する）1 と、この管理サーバ 1 を操作する端末である操作端末 A ～ E と、医療情報データベース 2 ～ 8 まで 7 種のデータベース（以下、「DB」と省略する）と、各医療情報 DB 2 ～ 8 を操作する端末である操作端末 2 0 ～ 8 0 とが設けられている。なお、ここで言う操作する端末とはデータベースに記憶される医療情報の閲覧、追加、修正及び加工することのできるものを指す。

【 0 0 3 1 】

管理サーバ 1 は、医療情報を一元管理するための装置であり、ネットワーク L を介して接続された操作端末 A ～ E により、データベース 1 6 に記憶される医療情報の閲覧、追加、修正及び加工することができる。医療情報 DB 2 ～ 8 は、管理サーバ 1 にネットワーク L を介して接続されており、操作端末 2 0 ～ 8 0 により、データベースに記憶される医療情報を閲覧、追加、修正及び加工することができる。また、医療情報 DB 2 ～ 8 に接続された操作端末 2 0 ～ 8 0 により、管理サーバ 1 にアクセスして医療情報の閲覧、追加、修正及び加工が可能となっている。

【 0 0 3 2 】

ここで、ネットワーク L は、サーバと、複数のク操作端末とを接続して構成され、接続されたサーバ及び複数の操作端末間で情報や資源（例えば、データベース、出力装置等）を共有するための、限られたエリア内におけるネットワークである。例えば、WWW（ワールド・ワイド・ウェブ）や TCP / IP などの、インターネットで普及している技術を使ってネットワーク L を構築することにより

、信頼性の高いネットワークをスピーディに構築できるとともに、インターネットとの親和性を高めることができる。なお、ネットワーク L は、情報管理の信頼性の観点から、特定のユーザのみアクセス可能なセキュリティを確保しているネットワークであることが望ましい。

【 0 0 3 3 】

なお、図 1 では 7 個の医療情報 DB 2 ～ 8 を一例として示したが、医療情報 DB は 2 個以上であれば特に制限はなく、医療情報 DB 2 ～ 8 に接続されている操作端末 2 0 ～ 8 0 についても、図 1 では一つのみ備える構成として記載したが 2 個以上又は複数個設置しても良い。また、管理サーバ 1 に接続された操作端末 A ～ E を 5 個として記載したが、管理サーバ 1 を操作する端末として各種医療情報 DB 2 ～ 8 に接続された操作端末 2 0 ～ 8 0 で代用しても良いし、直接バス等により接続された端末を 1 個あるいは 2 個以上備える構成であっても良い。

【 0 0 3 4 】

図 2 は、図 1 同様に医療情報を一元管理している医療情報管理システム 2 0 0 のシステム構成の一例を示す図である。この医療情報管理システム 2 0 0 は、地域医療情報化を目的とするものであり、各種医療機関 A ～ G で運用されているデータベースがネットワーク N により接続され、医療情報統括管理サーバ（以下、「管理サーバ」と記す）1 b により一元管理されている。図 2 に示すように、それぞれの医療機関 A ～ G に備えられるの 7 種のデータベースが有り、この医療機関 DB a ～ g を操作する操作端末 a 1 ～ g 1 が設けられている。なお、ここで言う操作する端末とはデータベースの医療情報を閲覧、追加、修正及び加工できるものであり、例えば、医療機関 DB a を操作する操作端末としては操作端末 a 1 、操作端末 a 2 、操作端末 a 3 ……操作端末 a N のように複数個設置してあっても良い。

【 0 0 3 5 】

管理サーバ 2 は、医療情報管理システム 2 0 0 の医療情報を一元管理するための装置であり、管理サーバ 2 に接続された操作端末 $\alpha \sim \varepsilon$ の操作により、医療情報の閲覧、追加、修正及び加工が可能となっている。また、医療機関 DB a ～ g は、管理サーバ 2 にネットワーク N を介して接続され、操作端末 a N ～ g N の操

作により、管理サーバ2にアクセスして、医療情報の閲覧、追加、修正及び加工が可能となっている。

【0036】

ここで、ネットワークNは、電話回線網、ISDN回線網、専用線、移動体通信網、通信衛星回線、CATV回線網等の各種通信回線と、それらを接続するインターネットサービスプロバイダ基地局等を含む。なお、ネットワークNは、任意な時に接続が可能であればよく、常時接続されている必要はない。また、ネットワークNは、情報管理の信頼性の観点から、特定のユーザのみアクセス可能なセキュリティを確保しているネットワークであることが望ましい。特に、管理サーバ2と管理サーバ2を操作する操作端末 $\alpha \sim \varepsilon$ との接続は、専用回線により構築されていることが好ましい。操作端末 $\alpha \sim \varepsilon$ は、管理サーバ2の医療情報を直接操作可能な端末だからである。

【0037】

なお、操作端末aN～操作端末gNは、前記管理サーバ2にアクセスして、医療情報の追加、変更、閲覧が可能な操作端末としても良い。また、図2では医療機関DBa～gを7個備える場合を例として記載したが、2個以上であれば特に制限はない。また、管理サーバ2にネットワークNを接続された操作端末 $\alpha \sim \varepsilon$ を5個備える場合を例として記載したが、管理サーバ2を操作する端末として各種医療機関A～Gの各DBに接続された操作端末aN～gNを代用しても良く、直接接続された端末が1個又は2個以上であっても良い。

【0038】

以上、2つの医療情報管理システムのシステム構成について説明を行ったが、上述した医療情報管理システム100、200は一例であり、その他種々の形態により構成されていても良い。なお、医療情報管理システム100を構成する各部と、医療情報管理システム200を構成する各部は、略同一の構成及び動作によってなるため、以下では、医療情報管理システム100に本発明が適用された場合を例として第1から第7の実施の形態について説明を行う。

【0039】

[第1の実施の形態]

まず、医療情報管理システム100における管理サーバ1aについて説明する。図3は、医療情報管理システム100における管理サーバ1aの要部構成を示すブロック図である。なお、図3では、本第1の実施の形態に必要な構成のみを示し、説明に不要なその他の構成及び装置については省略している。

【0040】

図3に示すように、管理サーバ1aは、制御部11、個人照合手段12、データアクセス権確認手段13、出力許可手段14、受信手段15、データベース16等を備えて構成されており、各部はバスにより接続されている。また、管理サーバ1aは、ネットワークLを介して接続される、管理サーバ1aを操作するための操作端末A～E及び管理サーバ1a内の医療情報をハードコピーとして出力するための出力装置x～zを備えている。

【0041】

制御部11は、データベース16内の記憶装置（図示せず）に記憶されている各種システムプログラムを読み出して実行し、管理サーバ1の各部を駆動制御する。具体的に、制御部11は、後述する情報蓄積処理1（図4参照）、情報利用処理1（図5参照）を実行する。この情報蓄積処理1を実行するに際して、制御部11は、医療情報DB2～6から送信される医療情報を受信すると、受信した医療情報から患者情報を抽出して、データベース16内で同一の患者に関する医療情報があるかを検索する。そして、データベース16内に同一の患者に関する医療情報がある場合、受信した医療情報を患者情報に対応付けて、既に記憶されている医療情報と統合してデータベース16に記憶させる。

【0042】

また、情報利用処理1を実行するに際して、制御部11は、操作端末A～Eからアクセス要求が送信されると、アクセス要求に含まれる操作端末A～Eの操作者の個人情報を抽出して、個人照合手段12により個人認証を行わせる。個人認証が成功した場合、データアクセス権確認手段13により指示された医療情報が利用可能な情報であるかを確認させ、当該医療情報が利用可能な情報である場合、医療情報の閲覧、追加、修正又は加工等を行わせる。さらに、操作端末A～Eから医療情報を出力する指示が入力された場合、制御部11は、出力許可手段1

5により、指示された医療情報が出力可能な情報であることを確認させ、当該医療情報が出力可能な情報である場合、出力許可手段15を介して出力装置x～zに出力させる。

【0043】

個人照合手段12は、操作端末A～EからネットワークNを介して送信されたアクセス要求を受信する。また、操作端末A～Eを操作する操作者の個人情報をアクセス要求から取得して、この個人情報に基づいて操作端末A～Eの操作者がアクセス可能な操作者であるかを判別する。ここで、個人情報は、個人を特定するための情報として、パスワード、IDカード情報、指紋、声紋、顔（輪郭等）、署名筆跡、虹彩パターン、眼底パターンあるいは静脈（血管）パターン等を含んでおり、予めデータベース16にアクセス可能な操作者として登録されている個人情報と比較して、個人の認証を行う。

【0044】

個人照合手段12は、パスワード、IDカード、指紋、掌紋、声紋、顔（輪郭等）、署名筆跡、虹彩パターン、眼底パターンあるいは静脈（血管）パターンを照合させる手段の中から選ばれる少なくとも1種の個人照合手段であることが好ましく、この中で指紋、声紋あるいは虹彩パターンのように個人特有の情報を照合させる手段がセキュリティの面からより好ましい。また、さらにセキュリティを向上させるためには個人照合手段12としてパスワードまたはIDカードによる認証と、指紋、声紋あるいは虹彩パターンを照合させる手段の中から選ばれる少なくとも1種の認証とを組み合わせた個人照合手段であることがより好ましい。

【0045】

これにより、種々の情報に基づいて操作者の個人認証を確実に行うことができ、医療情報管理システムのセキュリティを向上することができる。あるいは、複数の個人照合手段を組み合わせることにより、第三者による不正なシステムへの進入を確実に防ぐことができる。また、種々の個人照合手段を適用可能にすることにより汎用性の高いシステムを提供することができる。

【0046】

なお、アクセス可能な操作者としては、各種医療機関にいる医師、放射線技師、看護婦、薬剤師、病院の会計などを行う病院関係者、栄養士、訪問介護等を行うヘルパーあるいは患者等であり、管理サーバ1aに蓄積された医療情報を必要とする者の中から任意に登録することができる。なお、個人照合手段12は、個人照合するための装置を操作端末A～Eに備えることにより、管理サーバ1に接続される前に操作端末A～Eの個人照合手段12により個人認証される構成であってもよい。この場合、データアクセス権確認手段に受信手段を備える構成とし、操作端末A～Eの個人照合手段12で認証特定された操作者の指示により、操作端末A～Eから直接データアクセス権確認手段にアクセス要求が送信されても良い。

【0047】

データアクセス権確認手段13は、データベース16に記憶されている医療情報のうち、閲覧、追加、修正あるいは加工が許可されている医療情報を識別する。ここで、閲覧、追加、修正あるいは加工できる医療情報としては、臨床検査管理システムデータ、放射線科情報システムデータ、病院情報システムデータ、電子カルテシステムデータ、症例管理システム、薬歴管理システムデータ、医薬品文書データ、介護保険システムデータおよび医療関連文献データから選ばれる少なくとも1種のデータであり、より好ましくは前述のデータの中から選ばれる2種以上のデータである。

【0048】

データアクセス権確認手段13は、個人照合手段12により取得された操作者の個人情報に基づいてアクセス可能な医療情報を識別する構成であっても良く、例えば、医師、放射線技師、看護婦、薬剤師および病院の会計などを行う病院関係者のみが操作者である場合においては、アクセス可能な医療情報として、臨床検査管理システムデータ、放射線科情報システムデータ、病院情報システムデータ、電子カルテシステムデータ、症例管理システムデータ、および薬歴管理システムデータの中から選ばれる2種以上のデータであることがより好ましい。

【0049】

また、個人照合手段12により個人認証された操作者が、閲覧、追加、修正あ

るいは加工できるデータの種類としては、文字データ、オンオフデータ、静止画像データ、動画データの中から選ばれる少なくとも1種のデータであることが好ましい。また、この中で追加、修正あるいは加工できるデータが文字データあるいはオンオフデータである場合、操作端末A～Eに備えられる入力手段（図示せず）は、ペン入力、キーボード入力、マウス入力あるいは音声入力から選ばれる少なくとも1種の入力手段であり、操作端末A～Eを操作する者の習熟度によって適宜選択して用いることができる。なお、オンオフデータとは、情報をオン／オフにより示すデータであり、例えば、二者択一の情報である性別や病歴の有無等を示すデータである。

【 0 0 5 0 】

出力許可手段14は、管理サーバ1内の医療情報を別の記録媒体に電子情報として記録あるいは医療情報を印刷媒体にハードコピーとして出力することを許可するか否かを、前記個人照合手段12で得られた個人情報や、データアクセス権確認手段13の判別結果に基づいて判別する。

【 0 0 5 1 】

受信手段15は、複数の医療情報DB2～6の自動送信手段21～61から送信される医療情報を受信する。なお、自動送信手段21～61から送信される医療情報については、後述して詳細を説明する。

【 0 0 5 2 】

データベース16は、プログラムやデータ等があらかじめ記憶されている記録媒体（図示せず）を有しており、この記録媒体は磁氣的、光学的記録媒体、若しくは半導体メモリで構成されている。この記録媒体はデータベース16に固定的に設けられるもの、若しくは着脱自在に装着するものであり、この記録媒体には、システムプログラム、当該システムに対応する各種処理プログラム、及び各種処理プログラムで処理されたデータ等を記憶する。プログラムは、コンピュータが読み取り可能なプログラムコードの形態で格納され、制御部11は、当該プログラムコードに従った動作を逐次実行する。

【 0 0 5 3 】

また、記録媒体に記憶するプログラム、データ等は、その一部若しくは全部を

サーバやクライアント等の他の機器からWAN、LAN等のネットワーク回線の伝送媒体を介して受信手段15から受信して記憶する構成にしてもよく、さらに、記録媒体はネットワーク上に構築されたサーバの記録媒体であってもよい。また、前記プログラムをネットワーク回線等の伝送媒体を介してサーバやクライアントへ伝送してこれらの機器にインストールするように構成してもよい。

【0054】

具体的に、データベース16は、医療情報DB2～6から送信された医療情報を記憶しており、例えば、臨床検査管理システムデータ、放射線科情報システムデータ、病院情報システムデータ、電子カルテシステムデータ、症例管理システムデータ、薬歴管理システムデータ、医薬品文書データ、介護保険システムデータ、医療関連文献データ等を含んでいる。これらの医療情報は、医療情報DB2～6から送信される医療情報に付帯する患者情報に基づいて、患者毎に統合されて管理、蓄積されている。この患者情報は、患者を特定できる情報として、氏名、年齢、住所等の保険証に記載された情報のほかに、指紋、声紋、顔（輪郭等）、署名筆跡、虹彩パターン、眼底パターン、静脈（血管）パターン、歯科情報等を含んでいる。また、データベース16に記憶される医療情報に、追加、修正あるいは加工が行われた場合は、その操作結果を記憶する。

【0055】

また、データベース16は、管理サーバ1aにアクセス可能な操作者として登録されている個人の個人情報を記憶している。この個人情報には、個人を特定するための情報として、パスワード、IDカード情報、指紋、声紋、顔（輪郭等）、署名筆跡、虹彩パターン、眼底パターンあるいは静脈（血管）パターン等を含み、個人照合手段12により、管理サーバ1aにアクセス要求を送信した操作端末A～Eの操作者の認証を行う際に利用される。

【0056】

端末装置A～Eは、ネットワークNを介して管理サーバ1に接続され、管理サーバ1に記憶される医療情報の閲覧、追加、修正あるいは加工をするための操作指示を含むアクセス要求を管理サーバ1に送信する。このアクセス要求には、操作者の個人認証を行うための個人情報を含んでおり、この個人情報に基づいて操

作者がアクセス可能な個人であるか否かが認証される。そして、認証に成功した場合、操作指示が受け付けられる構成となっている。また、端末装置A～Eは、医療情報を出力装置x～zから出力させるための出力指示を管理サーバ1に送信する。

【0057】

出力装置x～zは、ネットワークLを介して、管理サーバ1、端末装置A～Eと接続されている。この出力装置x～zは、例えば、CD-R、CD-RW、DVD-R、DVD-RW、ハードディスク、Blu-ray Disc、特開2002-83431号公報、特開2002-123948号公報、特開2002-123949号公報、特開2002-183975号公報等に記載されている装置に用いられる高容量のホログラムメディア等への記録媒体への出力、サーマル銀塩記録メディア、フォトサーマル銀塩記録メディア、熱拡散性色素転写メディア、インクジェットメディアあるいは電子写真方式に用いられる記録メディア等の可視化情報やハードコピーとしての出力装置を適時選択して用いることができる。

【0058】

次に、医療情報DB2～6について説明する。

医療情報DB2～6（以下、統括的に「医療情報DB2」として示す）は、操作端末20～60（以下、統括的に「操作端末20」として示す）により操作され、操作端末20の入力部（図示せず）を介して入力された医療情報のうち、必要な情報を管理サーバ1aに自動で送信する自動送信手段21～61（以下、統括的に「自動送信手段21」として示す）を備えている。

【0059】

具体的に、この自動送信手段21により管理サーバ1aに送信される医療情報は、臨床検査管理システムデータ、放射線科情報システムデータ、病院情報システムデータ、電子カルテシステムデータ、症例管理システム、薬歴管理システムデータ、医薬品文書データ、介護保険システムデータ、医療関連文献データから選ばれる少なくとも1種のデータであり、より好ましくは前述のデータの中から選ばれる2種以上のデータである。さらに、医師、放射線技師、看護婦、薬剤師

および病院の会計などを行う病院関係者のみが使用する場合においては、臨床検査管理システムデータ、放射線科情報システムデータ、病院情報システムデータ、電子カルテシステムデータ、症例管理システムデータおよび薬歴管理システムデータから選ばれる２種以上のデータであることがより好ましい。

【 0 0 6 0 】

また、自動送信手段 2-1 は、端末装置 2 0 を介して入力され、医療情報 DB 2 に蓄積された医療情報を自動的に管理サーバ 1 に送信して蓄積させるが、この際、管理サーバ 1 a におけるデータ処理を簡便にする目的で、送信される医療情報のうち、過去に管理サーバ 1 へ送信された医療情報との差分を検出し、追加または変更されている医療情報のみを管理サーバ 1 へ送信する。例えば、図 3 に示すように、医療情報 DB 2 においては、データベースに記憶されている医療情報として、a 1 + b 1 が示されているが、そのうち必要な情報として a 1 のみがネットワークを介して管理サーバ 1 a に送信される。また、他の医療情報 DB 3 ~ 6 における医療情報 a 3 ~ a 6 についても同様にネットワークを介して管理サーバ 1 に送信され、医療情報が蓄積される。

【 0 0 6 1 】

また、自動送信手段 2 1 は、管理サーバ 1 a へ医療情報を送信してデータベース 1 6 に蓄積させる際に、送信する医療情報に情報を作成した作成日時を付帯情報として付与する構成であっても良い。これにより、管理サーバ 1 a の制御部 1 1 は、送信された医療情報の作成日時と、前回の送信され蓄積されている医療情報の作成日時とを照合し、新たに追加または変更されている医療情報のみをデータベース 1 6 に蓄積させることができ、情報処理を簡便に行うことができる。

【 0 0 6 2 】

なお、自動送信手段 2 1 により、医療情報 DB 2 から管理サーバ 1 a に医療情報が送信される時間は、個々のデータベースを構成するサーバやバックアップなどのシステム構成によって異なるが、医療情報 DB 2 の使用頻度が少ない時間帯、例えば深夜から早朝に掛けて送信するのが好ましい。

【 0 0 6 3 】

端末装置 2 0 は、医療情報 DB 2 を操作するための端末であり、医療情報 DB

2に記憶される医療情報の閲覧、追加、修正及び加工を行う装置である。また、端末装置20は、ネットワークNを介して管理サーバ1aに接続されており、管理サーバ1aに記憶される医療情報の閲覧、追加、修正及び加工を行うことも可能である。この場合も、端末装置20はアクセス要求と共に、操作者の個人情報を管理サーバ1aに送信し、認証が成功した場合に、アクセス要求が受け付けられる構成となっている。

【0064】

次に、本第1の実施の形態における動作について説明する。

動作説明の前提として、以下のフローチャートに記述されている各処理を実現するためのプログラムは、コンピュータが読み取り可能なプログラムコードの形態でデータベース16に格納されており、制御部11は、当該プログラムコードに従った動作を逐次実行する。また、制御部11は、伝送媒体を介して外部から供給されるプログラム及びデータを利用して、本実施の形態特有の動作を逐次実行することも可能である。

【0065】

図4は、制御部11により実行される情報蓄積処理1を示すフローチャートである。図4に示すように、制御部11は、受信手段15を介して医療情報DB2から医療情報を受信すると（ステップS1）、受信した医療情報から患者情報を抽出して（ステップS2）、データベース16内において、同一の患者に関する医療情報を検索する（ステップS3）。そして、同一の患者に関する医療情報がデータベース16にある場合、これらの医療情報を統合して、データベース16に記憶させ（ステップS4）、本情報蓄積処理を終了する。

【0066】

次に、図5は、制御部11により実行される情報利用処理1を示すフローチャートである。図5に示すように、制御部11は、個人認証手段12を介してアクセス要求を受信すると（ステップS11）、個人認証手段12により、個人情報を抽出させて、アクセス要求を送信してきた端末A～Eを操作する操作者の個人認証を行う（ステップS12）。次いで、個人認証が成功した場合（ステップS13；YES）、制御部11は、データアクセス権確認手段13により、アクセ

ス要求された医療情報が、アクセス可能な情報であるか否かを判断する（ステップS14）。

【0067】

アクセス要求された医療情報がアクセス可能な情報である場合（ステップS14；YES）、制御部11は、アクセス要求にしたがって、データベース16に記憶される医療情報の閲覧、追加、修正あるいは加工を行わせる（ステップS15）。さらに、制御部11は、端末装置A～Eを介して、医療情報の出力指示が入力された場合（ステップS16；YES）、出力許可手段14により、指示された医療情報が出力可能な情報であるかを判断させる（ステップS17）。そして、医療情報が出力可能な情報である場合、制御部11は、出力許可手段14を介して、当該医療情報を出力装置x～zに出力させ（ステップS18）、本情報利用処理を終了する。

【0068】

以上のように、管理サーバ1aは、医療情報DB2の自動送信手段21から自動送信される医療情報を、患者情報に基づいて患者毎に蓄積して管理するため、医療情報管理システム100内の医療情報を一括して管理することができ、管理サーバ1に重複した医療情報が蓄積されることがない。これにより、医療情報管理システム100の資源を有効に利用して、効率の良い医療情報の管理を行うことができる。

【0069】

また、この管理サーバ1aに蓄積された医療情報を利用するためには、個人照合手段12により、操作端末A～Eの操作者の個人認証を行い、この個人照合手段12により認証特定された操作者がアクセス可能な医療情報をデータアクセス権確認手段13により確認した上で、医療情報へのアクセスを許可する。これにより、第三者は、管理サーバ1aに記憶される医療情報に許可なくアクセスすることができない構成となり、管理サーバ1の医療情報を故意に閲覧、追加、修正あるいは加工するような不正行為を防止することができ、管理サーバ1aに記憶される医療情報の信頼性を向上させることができる。

【0070】

さらに、記録媒体に電子情報として記録あるいは印刷媒体にハードコピーとして出力する指示が入力された場合は、出力許可手段 1 4 により、指示された医療情報が出力可能な情報であるかを判断して医療情報の出力が許可された場合に、出力装置 x～z に出力させる。したがって、患者の個人情報の外部への流失や医療情報の別の記録媒体へのコピーを防止することができ、プライバシーの侵害を防いで、情報管理のセキュリティを向上させることができる。

【 0 0 7 1 】

なお、図 3 では管理サーバ 1 に必要な情報を自動的にデータ送信する複数の医療情報 DB として 5 個の医療 DB 2～6 を記載したが 2 種以上であれば特に制限はない。また、図 3 では管理サーバ 1 を操作する操作端末 A～E を 5 個備える構成にしたが、これらは必要に応じて複数用意することができ、操作端末 A～E はネットワーク L を介して、さらにはインターネットを介して用途に応じて種々の場所に設置することができる。さらに、前述の図 1 あるいは図 2 で説明した様に医療情報 DB 2～8 に設けられている操作端末 2 0～8 0、医療機関 DB a～g に設けられている操作端末 a 1～g 1 を用いて前記管理サーバ 1 a、1 b にアクセスして追加、変更、閲覧が可能な構成としても良い。加えて出力装置 x～z においても図 3 では 3 個で記載したが 1 個以上であれば特に制限はなく、また出力装置自体もネットワーク L を介して他の場所に設置されていても良く、操作端末 A～E に接続する形で出力装置 x～z が接続されていても良い。なお、後述で説明する第 2 から第 7 の実施の形態においても同様である。

【 0 0 7 2 】

[第 2 の実施の形態]

次に、本発明を適用した第 2 の実施の形態について説明する。

図 6 は、本第 2 の実施の形態における管理サーバ 1 b の要部構成を示すブロック図である。図 6 に示すように、管理サーバ 1 b は、制御部 1 1、個人照合手段 1 2、データアクセス権確認手段 1 3、受信手段 1 5、データベース 1 6、データ改竄防止手段 1 7 等を備えて構成されている。すなわち、管理サーバ 1 b は、上述した第 1 の実施の形態における管理サーバ 1 a と比較して、出力許可手段 1 4 の代わりに、データ改竄防止手段 1 7 を新たに備える構成となっている。なお

、データ改竄防止手段 1 7 を除く各構成部分については、上述した第 1 の実施の形態における管理サーバ 1 a と同一の構成によってなるため、同一の構成部分については詳細な説明を省略する。以下では、本第 2 の実施の形態に特徴的な構成及び動作について説明する。

【 0 0 7 3 】

データ改竄防止手段 1 7 は、データベース 1 6 に記憶される医療情報に追加、修正あるいは加工する場合において、元の情報は保持したまま、元の情報への変更を履歴として記憶することにより、医療情報が改竄されることを防止する。これにより、誤って大事な医療情報を書き換えてしまう事を防止するとともに、データベース 1 6 の医療情報を故意に追加、修正あるいは加工するような不正行為を防止でき、蓄積された医療情報のセキュリティを確保することができる。

【 0 0 7 4 】

次に、本第 2 の実施の形態における動作を説明する。管理サーバ 1 c の制御部 1 1 は、本第 2 の実施の形態に特徴的な処理として情報利用処理 2 を実行する。図 7 は、制御部 1 1 により実行される情報利用処理 2 を示すフローチャートである。図 7 に示すように、制御部 1 1 は、個人認証手段 1 2 を介してアクセス要求を受信すると（ステップ S 2 1）、個人認証手段 1 2 により、個人情報を出出させて、アクセス要求を送信してきた端末 A ～ E を操作する操作者の個人認証を行う（ステップ S 2 2）。次いで、個人認証が成功した場合（ステップ S 2 3；YES）、制御部 1 1 は、データアクセス権確認手段 1 3 により、アクセス要求された医療情報が、アクセス可能な医療情報であるか否かを判断する（ステップ S 2 4）。

【 0 0 7 5 】

次いで、アクセス要求された医療情報がアクセス可能な情報である場合（ステップ S 2 4；YES）、制御部 1 1 は、アクセス要求にしたがって、データベース 1 6 に記憶される医療情報の閲覧や、医療情報に対する追加、修正又は加工を行わせる（ステップ S 2 5）。制御部 1 1 は、データベース 1 6 に記憶される医療情報に追加、修正又は加工が行われた場合、データ改竄防止手段 1 7 により、これらの変更履歴を当該医療情報に対応付けて記憶させる（ステップ S 2 6）。

そして、制御部 1 1 は、医療情報への追加、修正又は加工が終了したか否かを判別し（ステップ S 2 7）、医療情報の変更が終了した場合は（ステップ S 2 7；YES）、本情報利用処理 2 を終了する。また、医療情報の変更が終了していない場合（ステップ S 2 7；NO）、制御部 1 1 は、ステップ S 2 5 に移行して、上述した処理を繰り返して実行する。

【0 0 7 6】

以上のように、本第 2 の実施の形態において、管理サーバ 1 b は、データ改竄防止手段 1 7 により、管理サーバ 1 b のデータベース 1 6 に記憶される医療情報に追加、修正又は加工が行われた場合、元の医療情報を保持したまま、この変更履歴を当該医療情報に対応付けて記憶する。これにより、データベース 1 6 に記憶される医療情報が書き換えられたり、不正に改竄されることを防いで、医療情報の信頼性を向上させることができる。また、元の医療情報が保持されたまま、変更履歴が記憶されるため、例えば、医療事故等が発生した場合に、不都合な記録が消去され、情報が隠蔽されてしまうことがない。

【0 0 7 7】

〔第 3 の実施の形態〕

次に、本発明を適用した第 3 の実施の形態について説明する。

図 6 は、本第 2 の実施の形態における管理サーバ 1 c の要部構成を示すブロック図である。図 6 に示すように、管理サーバ 1 c は、制御部 1 1、個人照合手段 1 2、データアクセス権確認手段 1 3、受信手段 1 5、データベース 1 6、日付日時付与手段 1 8 等を備えて構成されている。すなわち、管理サーバ 1 c は、上述した第 1 の実施の形態における管理サーバ 1 a と比較して、出力許可手段 1 4 の代わりに、日付日時入力手段 1 8 を新たに備える構成となっている。なお、日付日時付与手段 1 8 を除く各構成部分については、上述した第 1 の実施の形態における管理サーバ 1 a と同一の構成によってなるため、同一の構成部分については詳細な説明を省略する。以下では、本第 3 の実施の形態に特徴的な構成及び動作について説明する。

【0 0 7 8】

日付日時付与手段 1 8 は、前記複数の医療情報 DB 2 ～ 6 から医療情報が送信

され、受信手段15により受信した日時を付帯情報として付与する。また、管理サーバ1cのデータベース16に記憶される医療情報の閲覧、追加、修正又は加工された日時を付帯情報として付与する。なお、日付日時付与手段18は、受信手段15により受信された情報がデータベース16に記憶された日時を付帯情報として付与する構成であっても良い。

【0079】

これにより、管理サーバ1cに新規の医療情報が送信又は記憶された履歴や、管理サーバ1cのデータベース16に記憶される医療情報が閲覧、追加、修正又は加工された履歴を過去にさかのぼって確認することができ、蓄積された医療情報の変遷を容易に把握することができる。これにより、例えば、医療情報が臨床検査管理システムデータ、放射線科情報システムデータ、病院情報システムデータ、電子カルテシステムデータ、症例管理システムデータおよび薬歴管理システムデータ等である場合、患者の状態の変化を時系列に従って観察することができ、医師による診断精度及び診断効率を向上させることができる。

【0080】

次に、本第3の実施の形態における動作を説明する。制御部11は、本第3の実施の形態に特徴的な処理として後述する情報蓄積処理2（図9参照）及び情報利用処理3（図10参照）を実行する。

【0081】

図9は、制御部11により実行される情報蓄積処理2を示すフローチャートである。図9に示すように、制御部11は、受信手段15を介して医療情報DB2から医療情報を受信すると（ステップS31）、日付日時付与手段18により、受信日時を取得して、受信した医療情報に付帯情報として付与させる（ステップS32）。

【0082】

次いで、制御部11は、受信した医療情報から患者情報を抽出して（ステップS33）、データベース16において、同一の患者に関する医療情報を検索する（ステップS34）。そして、同一の患者に関する医療情報がデータベース16にある場合、これらの医療情報を統合して、付帯情報とともにデータベース16

に記憶させ（ステップS35）、本情報蓄積処理2を終了する。

【0083】

図10は、制御部11により実行される情報利用処理3を示すフローチャートである。図10に示すように、制御部11は、個人認証手段12を介してアクセス要求を受信すると（ステップS41）、個人認証手段12により、個人情報を抽出させて（ステップS42）、アクセス要求を送信してきた端末A～Eを操作する操作者の個人認証を行う。次いで、個人認証が成功した場合（ステップS43；YES）、制御部11は、データアクセス権確認手段13により、アクセス要求された医療情報が、アクセス可能な情報であるか否かを判断する（ステップS44）。

【0084】

次いで、アクセス要求された医療情報がアクセス可能な情報である場合（ステップS44；YES）、制御部11は、アクセス要求にしたがって、データベース16に記憶される医療情報の閲覧や、医療情報に対する追加、修正又は加工を行わせる（ステップS45）。そして、制御部11は、日付日時付与手段18により、医療情報の閲覧、追加、修正又は加工が行われた日時を取得し、付帯情報として当該医療情報に対応付けてデータベース16に記憶させ（ステップS46）、本情報利用処理3を終了する。

【0085】

以上のように、本第3の実施の形態において、管理サーバ1cは、日付日時付与手段18により、データベース16に新規な医療情報が記憶された日時や、データベース16に記憶される医療情報の追加、修正又は加工された日時を、当該医療情報に付与する。これにより、医療情報の変遷を時系列に基づいて確認することができ、患者の状態の変化を的確に把握することができ、医師の診断精度及び診断効率を向上させることができる。また、医療情報を追加、修正又は加工した日時が限定されることにより、不正に医療情報を操作する行為を抑制する効果が得られる。

【0086】

[第4の実施の形態]

次に、本発明を適用した第 4 の実施の形態について説明する。

図 1 1 は、本第 4 の実施の形態における管理サーバ 1 d の要部構成を示すブロック図である。図 1 1 に示すように、管理サーバ 1 d は、制御部 1 1、個人照合手段 1 2、データアクセス権確認手段 1 3、出力許可手段 1 4、受信手段 1 5、データベース 1 6、データ改竄防止手段 1 7 等を備えて構成されている。すなわち、管理サーバ 1 d は、上述した第 1 の実施の形態における管理サーバ 1 a と比較して、データ改竄防止手段 1 7 をさらに備える構成となっている。なお、各構成部分については、上述した第 1 の実施の形態における管理サーバ 1 a 又は第 2 の実施の形態における管理サーバ 1 b と同一の構成によってなるため、同一の構成部分については詳細な説明を省略する。以下では、本第 4 の実施の形態に特徴的な動作について説明する。

【 0 0 8 7 】

制御部 1 1 は、本第 4 の実施の形態に特徴的な処理として、後述する情報利用処理 4（図 1 2 参照）を実行する。図 1 2 は、制御部 1 1 により実行される情報利用処理 4 を示すフローチャートである。図 1 2 に示すように、制御部 1 1 は、個人認証手段 1 2 を介してアクセス要求を受信すると（ステップ S 5 1）、個人認証手段 1 2 により、個人情報を出出させて、アクセス要求を送信してきた端末 A～E を操作する操作者の個人認証を行う（ステップ S 5 2）。次いで、個人認証が成功した場合（ステップ S 5 3；YES）、制御部 1 1 は、データアクセス権確認手段 1 3 により、アクセス要求された医療情報が、アクセス可能な情報であるか否かを判断する（ステップ S 5 4）。

【 0 0 8 8 】

次いで、アクセス要求された医療情報がアクセス可能な情報である場合（ステップ S 5 4；YES）、制御部 1 1 は、アクセス要求にしたがって、データベース 1 6 に記憶される医療情報の閲覧や、医療情報に対する追加、修正又は加工を行わせる（ステップ S 5 5）。制御部 1 1 は、データベース 1 6 に記憶される医療情報に追加、修正又は加工が行われた場合、データ改竄防止手段 1 7 により、これらの変更履歴を当該医療情報に対応付けて記憶させる（ステップ S 2 6）。そして、制御部 1 1 は、医療情報への追加、修正又は加工が終了したか否かを判

別し（ステップ S 5 7）、これらの変更が終了した場合は（ステップ S 2 7；Y E S）、操作端末 A～E から出力指示が入力されたか否かを判別する（ステップ S 5 8）。

【0089】

端末装置 A～E を介して、医療情報の出力指示が入力された場合（ステップ S 5 8-; Y E S）、制御部 1 1 は、出力許可手段 1 4 により指示された医療情報が出力可能な情報であるかを判断させる（ステップ S 5 9）。そして、医療情報が出力可能な情報である場合、制御部 1 1 は、出力許可手段 1 4 を介して、当該医療情報を出力装置 x～z に出力させ（ステップ S 6 0）、本情報利用処理 4 を終了する。

【0090】

以上のように、本第 4 の実施の形態において、管理サーバ 1 d は、データ改竄防止手段 1 7 により、管理サーバ 1 d のデータベース 1 6 に記憶される医療情報に追加、修正又は加工が行われた場合、元の医療情報を保持したまま、この変更履歴を当該医療情報に対応付けて記憶する。また、出力許可手段 1 4 により、出力指示された医療情報が出力可能な情報であるかを判断し、医療情報の出力が許可された場合に、医療情報を出力させる。これにより、管理サーバ 1 の医療情報を故意に閲覧、追加、修正あるいは加工するような不正行為を防止するとともに、患者の個人情報の外部への流失や医療情報の別の記録媒体へのコピーを防止することができ、情報管理のセキュリティを向上させることができる。

【0091】

[第 5 の実施の形態]

次に、本発明を適用した第 5 の実施の形態について説明する。

図 1 3 は、本第 5 の実施の形態における管理サーバ 1 e の要部構成を示すブロック図である。図 1 3 に示すように、管理サーバ 1 e は、制御部 1 1、個人照合手段 1 2、データアクセス権確認手段 1 3、出力許可手段 1 4、受信手段 1 5、データベース 1 6、日付日時付与手段 1 8 等を備えて構成されている。すなわち、管理サーバ 1 e は、上述した第 1 の実施の形態における管理サーバ 1 a と比較して、日付日時付与手段 1 8 をさらに備える構成となっている。なお、各構成部

分については、上述した第 1 の実施の形態における管理サーバ 1 a 又は第 3 の実施の形態における管理サーバ 1 c と同一の構成によってなるため、同一の構成部分については詳細な説明を省略する。以下では、本第 5 の実施の形態に特徴的な動作について説明する。

【 0 0 9 2 】

制御部 1-1 は、本第 5 の実施の形態に特徴的な処理として、情報蓄積処理 2（図 9 参照）及び後述する情報利用処理 5（図 1 4 参照）を実行する。なお、情報蓄積処理 2 については、上述した第 3 の実施の形態における情報蓄積処理 2 と同一の処理であるため、説明を省略する。

【 0 0 9 3 】

図 1 4 は、制御部 1 1 により実行される情報利用処理 5 を示すフローチャートである。図 1 4 に示すように、制御部 1 1 は、個人認証手段 1 2 を介してアクセス要求を受信すると（ステップ S 6 1）、個人認証手段 1 2 により、個人情報を出出させて（ステップ S 6 2）、アクセス要求を送信してきた端末 A ～ E を操作する操作者の個人認証を行う。次いで、個人認証が成功した場合（ステップ S 6 3；Y E S）、制御部 1 1 は、データアクセス権確認手段 1 3 により、アクセス要求された医療情報が、アクセス可能な情報であるか否かを判断する（ステップ S 6 4）。

【 0 0 9 4 】

次いで、アクセス要求された医療情報がアクセス可能な情報である場合（ステップ S 6 4；Y E S）、制御部 1 1 は、アクセス要求にしたがって、データベース 1 6 に記憶される医療情報の閲覧や、医療情報に対する追加、修正又は加工を行わせる（ステップ S 6 5）。そして、制御部 1 1 は、日付日時付与手段 1 8 により、医療情報の閲覧、追加、修正又は加工が行われた日時を取得し、付帯情報として当該医療情報に付与させる（ステップ S 6 6）。

【 0 0 9 5 】

次いで、制御部 1 1 は、操作端末 A ～ E から出力指示が入力されたか否かを判別し（ステップ S 6 7）、医療情報の出力指示が入力された場合（ステップ S 6 7；Y E S）、出力許可手段 1 4 により、指示された医療情報が出力可能な情報

であるかを判断させる（ステップ S 6 8）。そして、医療情報が出力可能な情報である場合（ステップ S 6 8 ; Y E S）、制御部 1 1 は、出力許可手段 1 4 を介して、当該医療情報を出力装置 x ~ z に出力させ（ステップ S 6 9）、本情報利用処理 5 を終了する。

【 0 0 9 6 】

以上のように、本第 5 の実施の形態において、管理サーバ 1 e は、日付日時付与手段 1 8 により、データベース 1 6 に新規な医療情報が記憶された日時や、データベース 1 6 に記憶される医療情報の追加、修正又は加工された日時を、当該医療情報に対応付けて記憶させる。また、出力許可手段 1 4 により、出力指示された医療情報が出力可能な情報であるかを判断し、医療情報の出力が許可された場合に、医療情報を出力させる。

【 0 0 9 7 】

これにより、医療情報の変遷を時系列に基づいて確認することができ、患者の状態の変化を的確に把握することができ、医師の診断精度及び診断効率を向上させることができる。また、医療情報を追加、修正又は加工した日時が限定されることにより、データベース 1 6 の医療情報を過去にさかのぼって不正に操作する行為を抑制する効果が得られる。さらに、患者の個人情報の外部への流失や医療情報の別の記録媒体へのコピーを防止することができ、情報管理のセキュリティを向上させることができる。

【 0 0 9 8 】

〔第 6 の実施の形態〕

次に、本発明を適用した第 6 の実施の形態について説明する。

図 1 5 は、本第 6 の実施の形態における管理サーバ 1 f の要部構成を示すブロック図である。図 1 5 に示すように、管理サーバ 1 f は、制御部 1 1、個人照合手段 1 2、データアクセス権確認手段 1 3、受信手段 1 5、データベース 1 6、データ改竄防止手段 1 7、日付日時付与手段 1 8 等を備えて構成されている。すなわち、管理サーバ 1 f は、上述した第 1 の実施の形態における管理サーバ 1 a と比較して、出力許可手段 1 4 の代わりに、データ改竄防止手段 1 7 及び日付日時付与手段 1 8 をさらに備える構成となっている。なお、各構成部分については

、上述した第 1 の実施の形態における管理サーバ 1 a、第 2 の実施の形態における管理サーバ 1 b、第 3 の実施の形態における管理サーバ 1 c と同一の構成によってなるため、同一の構成部分については詳細な説明を省略する。以下では、本第 6 の実施の形態に特徴的な動作について説明する。

【 0 0 9 9 】

制御部 1 1 は、本第 6 の実施の形態に特徴的な処理として、情報蓄積処理 2（図 9 参照）及び後述する情報利用処理 6（図 1 6 参照）を実行する。なお、情報蓄積処理 2 については、上述した第 3 の実施の形態における情報蓄積処理 2 と同一の処理であるため、説明を省略する。

【 0 1 0 0 】

図 1 6 は、制御部 1 1 により実行される情報利用処理 6 を示すフローチャートである。図 1 6 に示すように、制御部 1 1 は、個人認証手段 1 2 を介してアクセス要求を受信すると（ステップ S 7 1）、個人認証手段 1 2 により、個人情報を出出させて（ステップ S 7 2）、アクセス要求を送信してきた端末 A ～ E を操作する操作者の個人認証を行う。次いで、個人認証が成功した場合（ステップ S 7 3；YES）、制御部 1 1 は、データアクセス権確認手段 1 3 により、アクセス要求された医療情報が、アクセス可能な情報であるか否かを判断する（ステップ S 7 4）。

【 0 1 0 1 】

次いで、アクセス要求された医療情報がアクセス可能な情報である場合（ステップ S 7 4；YES）、制御部 1 1 は、アクセス要求にしたがって、データベース 1 6 に記憶される医療情報の閲覧や、医療情報に対する追加、修正又は加工を行わせる（ステップ S 7 5）。制御部 1 1 は、日付日時付与手段 1 8 により、医療情報の閲覧、追加、修正又は加工が行われた日時を取得し、付帯情報として当該医療情報に付与させる（ステップ S 7 6）。さらに、データ改竄防止手段 1 7 により、これらの変更履歴を当該医療情報に対応付けてデータベース 1 6 に記憶させる（ステップ S 7 7）。

【 0 1 0 2 】

そして、制御部 1 1 は、医療情報への追加、修正又は加工が終了したか否かを

判別し（ステップ S 7 8）、医療情報の変更が終了した場合は（ステップ S 7 8；YES）、本情報利用処理 6 を終了する。また、医療情報の変更が終了していない場合（ステップ S 7 8；NO）、制御部 1 1 は、ステップ S 7 5 に移行して、上述した処理を繰り返して実行する。

【0103】

以上のように、本第 6 の実施の形態によれば、管理サーバ 1 e は、日付日時付与手段 1 8 により、データベース 1 6 に新規な医療情報が記憶された日時を付帯情報として当該医療情報に付与する。また、データ改竄防止手段 1 7 及び日付日時付与手段 1 8 により、データベース 1 6 に記憶される医療情報が追加、修正又は加工された場合、その変更履歴及び変更日時を当該医療情報に対応付けて記憶する。

【0104】

これにより、医療情報の変遷を時系列に基づいて確認することができ、患者の状態の変化を的確に把握することができ、医師の診断精度及び診断効率を向上させることができる。また、医療情報を追加、修正又は加工した日時及び変更履歴が限定されることにより、データベース 1 6 の医療情報を過去にさかのぼって不正に改竄されることを防いで、医療情報の信頼性を向上させることができる。

【0105】

[第 7 の実施の形態]

次に、本発明を適用した第 7 の実施の形態について説明する。

図 1 7 は、本第 6 の実施の形態における管理サーバ 1 g の要部構成を示すブロック図である。図 1 7 に示すように、管理サーバ 1 f は、制御部 1 1、個人照合手段 1 2、データアクセス権確認手段 1 3、出力許可手段 1 4、受信手段 1 5、データベース 1 6、データ改竄防止手段 1 7、日付日時付与手段 1 8 等を備えて構成されている。すなわち、管理サーバ 1 f は、上述した第 1 の実施の形態における管理サーバ 1 a と比較して、データ改竄防止手段 1 7 及び日付日時付与手段 1 8 をさらに備える構成となっている。なお、各構成部分については、上述した第 1 の実施の形態における管理サーバ 1 a、第 2 の実施の形態における管理サーバ 1 b、第 3 の実施の形態における管理サーバ 1 c と略同一の構成によってなる

ため、同一の構成部分については詳細な説明を省略する。以下では、本第 7 の実施の形態に特徴的な動作について説明する。

【0106】

制御部 11 は、本第 7 の実施の形態に特徴的な処理として、情報蓄積処理 2（図 9 参照）及び後述する情報利用処理 7（図 18 参照）を実行する。なお、情報蓄積処理 2 については、上述した第 3 の実施の形態における情報蓄積処理 2 と同一の処理であるため、説明を省略する。

【0107】

図 18 は、制御部 11 により実行される情報利用処理 7 を示すフローチャートである。図 18 に示すように、制御部 11 は、個人認証手段 12 を介してアクセス要求を受信すると（ステップ S81）、個人認証手段 12 により、個人情報抽出させて（ステップ S82）、アクセス要求を送信してきた端末 A～E を操作する操作者の個人認証を行う。個人認証が成功した場合（ステップ S83；YES）、制御部 11 は、データアクセス権確認手段 13 により、アクセス要求された医療情報が、アクセス可能な情報であるか否かを判断する（ステップ S84）。

【0108】

アクセス要求された医療情報がアクセス可能な情報である場合（ステップ S84；YES）、制御部 11 は、アクセス要求にしたがって、データベース 16 に記憶される医療情報の閲覧や、医療情報に対する追加、修正又は加工を行わせる（ステップ S85）。次いで、制御部 11 は、日付日時付与手段 18 により、医療情報の閲覧、追加、修正又は加工が行われた日時を取得し、付帯情報として当該医療情報に付与させる（ステップ S86）。また、制御部 11 は、データ改竄防止手段 17 により、これらの変更履歴を当該医療情報に対応付けて記憶させる（ステップ S87）。

【0109】

さらに、制御部 11 は、医療情報への追加、修正又は加工が終了したか否かを判別し（ステップ S88）、医療情報の変更が終了した場合（ステップ S88；YES）、操作端末 A～E から出力指示が入力されたか否かを判別する（ステッ

プ S 8 9)。操作端末 A～E から出力指示が入力された場合（ステップ S 8 9；Y E S）、制御部 1 1 は、出力許可手段 1 4 により、指示された医療情報が出力可能な情報であるかを判断させる（ステップ S 9 0）。そして、医療情報が出力可能な情報である場合（ステップ S 9 0；Y E S）、制御部 1 1 は、出力許可手段 1 4 を介して、当該医療情報を出力装置 x～z に出力させ（ステップ S 9 1）、本情報利用処理 7 を終了する。

【0 1 1 0】

以上のように、本第 7 の実施の形態において、サーバ 1 g は、日付日時付与手段 1 8 により、データベース 1 6 に新規な医療情報が記憶された日時を付帯情報として当該医療情報に付与させる。また、データ改竄防止手段 1 7 及び日付日時付与手段 1 8 により、データベース 1 6 に記憶される医療情報が追加、修正又は加工された場合、その変更履歴及び変更日時を当該医療情報に対応付けて記憶する。さらに、サーバ 1 g は、出力許可手段 1 4 により、出力指示された医療情報が出力可能な情報であるかを判断し、医療情報の出力が許可された場合に、医療情報を出力させる。

【0 1 1 1】

これにより、管理サーバ 1 g のデータベース 1 6 に記憶される医療情報を過去にさかのぼって、閲覧、追加、修正あるいは加工するような不正行為を防止するとともに、患者の個人情報の外部への流失や医療情報の別の記録媒体へのコピーを防止することができ、情報管理のセキュリティを向上させることができる。また、医療情報が新規に送信又は記憶された日時や、医療情報の更新された日時を記憶するため、医療情報の変遷が明確になり、患者の状態の変化を容易に確認できる。これにより、医師の診断効率、診断制度を向上させることができる。

【0 1 1 2】

なお、上述した第 1 から第 7 の実施の形態における記述は、本発明に係る医療情報管理システムの一例であり、これらに限定されるものではない。

【0 1 1 3】

例えば、管理サーバ 1 a～1 g に備えるデータベース 1 6 は、単一のハードディスクで形成されるか、単一のハードディスクに複数のボリュームあるいはパー

ティションを切ったものでも良く、さらには複数のハードディスクを並列に繋げたもの、複数の繋げた個々のハードディスクに複数のボリュームあるいはパーティションを切ったものでも良い。なお、必要な情報を短時間で送受信したり、ハードディスクがクラッシュした際の復旧の容易性あるいはバックアップの容易性の問題から、図 1 9 に示すように、データベース 1 6 に複数のデータベース A ～ E を備えて構成されるものが好ましい。この場合、制御部 1 1 は、操作端末 A ～ E から送信されるアクセス要求に応じて、データベース A ～ E から必要な医療情報を選択して取得する。

【 0 1 1 4 】

また、例えば、医療情報管理システム 2 0 0 において、管理サーバ 1、医療機関 D B a ～ g、操作端末 a 1 ～ g 1、操作端末 $\alpha \sim \varepsilon$ を接続するネットワークは、それぞれ専用回線により構築されることがセキュリティ上好ましいが、例えば、地域の中核となる病院とかかりつけ医などの小規模病院間の接続のように、専用回線で接続することが難しい場合においては、送受信する情報を暗号化することが情報の漏洩を防ぐ意味から好ましい。この場合、管理サーバ 1、医療機関 D B a ～ g、操作端末 a 1 ～ g 1、操作端末 $\alpha \sim \varepsilon$ に暗号化手段（図示せず）及び復号化手段（図示せず）を備え、例えば、秘密鍵暗号、公開鍵暗号等を用いて送受信する情報の暗号化及び復号化を行う。また、暗号化される情報は、医療情報に限らず、上述したアクセス要求に含まれる操作指示や操作者の個人情報等を含むことが好ましい。

【 0 1 1 5 】

その他、本第 1 から第 7 の実施の形態における医療情報管理システムにおける構成部分の細部構成、及び細部動作に関しては、本発明の趣旨を逸脱することのない範囲で適宜変更可能であることはもちろんである。

【 0 1 1 6 】

【発明の効果】

本発明によれば、統合的に医療情報が管理される医療情報管理システムにおいて、医療情報を操作する操作者の認証を行うとともに、認証された操作者により操作される医療情報が、操作可能な情報であることを確認することにより、医療情報

が不正に操作されることを防いで、情報管理のセキュリティを向上させることができる。また、医療情報を出力する際は、出力指示された医療情報が出力可能な情報であるかを確認した後に出力するため、重要な医療情報が外部に漏洩することを防止することができる。

【 0 1 1 7 】

さらに、医療情報に追加、修正あるいは加工等の操作が行われた場合は、元の医療情報を保持したまま、当該医療情報に対応付けて変更履歴を記憶するため、重要な医療情報が誤って書き換えられたり、不正に医療情報が改竄されることを防止できる。また、医療情報の記憶日時や変更された日時を付帯情報として医療情報に付与するため、これらの日時が限定されることにより、不正に情報を操作する行為を抑制する効果が得られる。

【図面の簡単な説明】

【図 1】

本発明を適用した医療情報管理システム 1 0 0 のシステム構成を示す概念図である。

【図 2】

本発明を適用した医療情報管理システム 2 0 0 のシステム構成を示す概念図である。

【図 3】

本発明を適用した第 1 の実施の形態における管理サーバ 1 a の要部構成を示すブロック図である。

【図 4】

図 3 に示す制御部 1 1 により実行される情報蓄積処理 1 を示すフローチャートである。

【図 5】

図 3 に示す制御部 1 1 により実行される情報利用処理 1 を示すフローチャートである。

【図 6】

本発明を適用した第 2 の実施の形態における管理サーバ 1 b の要部構成を示す

ブロック図である。

【図 7】

図 6 に示す制御部 1 1 により実行される情報利用処理 2 を示すフローチャートである。

【図 8】

本発明を適用した第 3 の実施の形態における管理サーバ 1 c の要部構成を示すブロック図である。

【図 9】

図 8 に示す制御部 1 1 により実行される情報蓄積処理 2 を示すフローチャートである。

【図 1 0】

図 8 に示す制御部 1 1 により実行される情報利用処理 3 を示すフローチャートである。

【図 1 1】

本発明を適用した第 4 の実施の形態における管理サーバ 1 d の要部構成を示すブロック図である。

【図 1 2】

図 1 1 に示す制御部 1 1 により実行される情報利用処理 4 を示すフローチャートである。

【図 1 3】

本発明を適用した第 5 の実施の形態における管理サーバ 1 e の要部構成を示すブロック図である。

【図 1 4】

図 1 3 に示す制御部 1 1 により実行される情報利用処理 5 を示すフローチャートである。

【図 1 5】

本発明を適用した第 6 の実施の形態における管理サーバ 1 f の要部構成を示すブロック図である。

【図 1 6】

図 1 5 に示す制御部 1 1 により実行される情報利用処理 6 を示すフローチャートである。

【図 1 7】

本発明を適用した第 7 の実施の形態における管理サーバ 1 g の要部構成を示すブロック図である。

【図 1 8】

図 1 7 に示す制御部 1 1 により実行される情報利用処理 7 を示すフローチャートである。

【図 1 9】

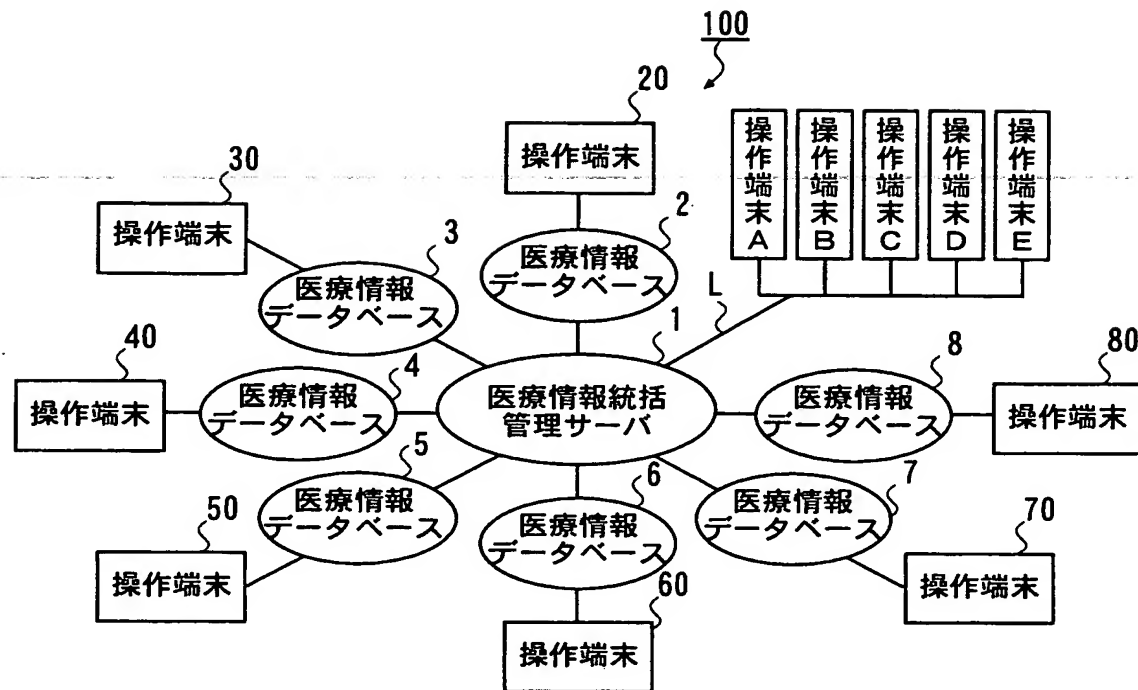
管理サーバ 1 のデータベース 1 6 のデータ構成の一例を示す図である。

【符号の説明】

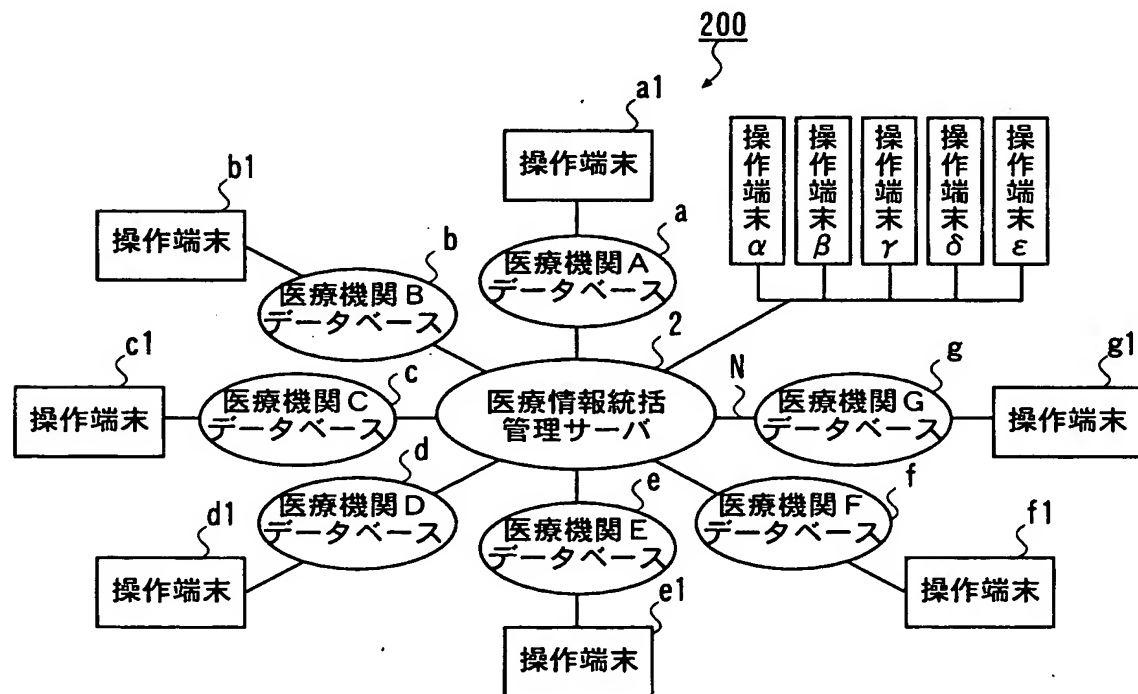
- 1 0 0 ~ 2 0 0 医療情報管理システム
- 1 a ~ 1 g、2 医療情報統括管理サーバ
- 1 1 制御部
- 1 2 個人照合手段
- 1 3 データアクセス権確認手段
- 1 4 出力許可手段
- 1 5 受信手段
- 1 6 データベース
- 1 7 データ改竄防止手段
- 1 8 日付日時付与手段
- 2 ~ 8 医療情報データベース
- 2 1 ~ 6 1 自動送信手段
- a ~ g 医療機関データベース
- A ~ E、 α ~ ε 操作端末
- L, N ネットワーク

【書類名】 図面

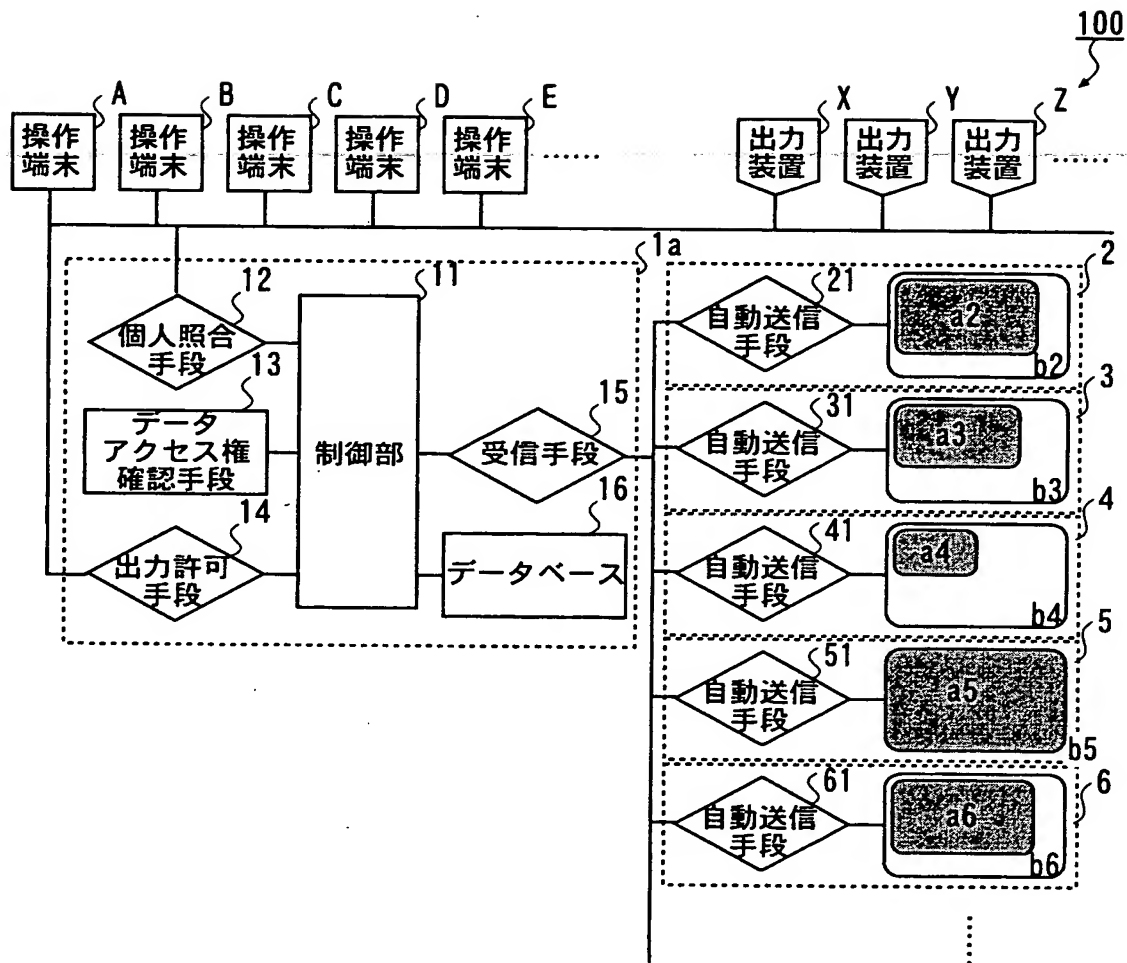
【図 1】



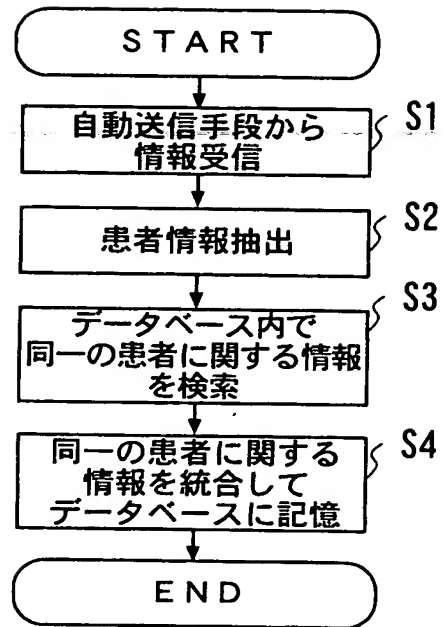
【図 2】



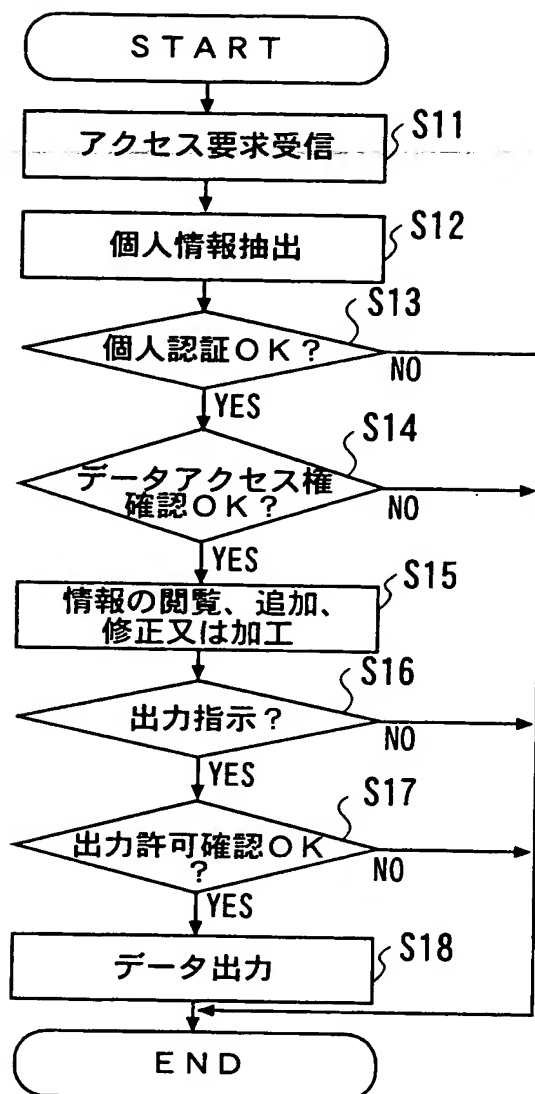
【図 3】



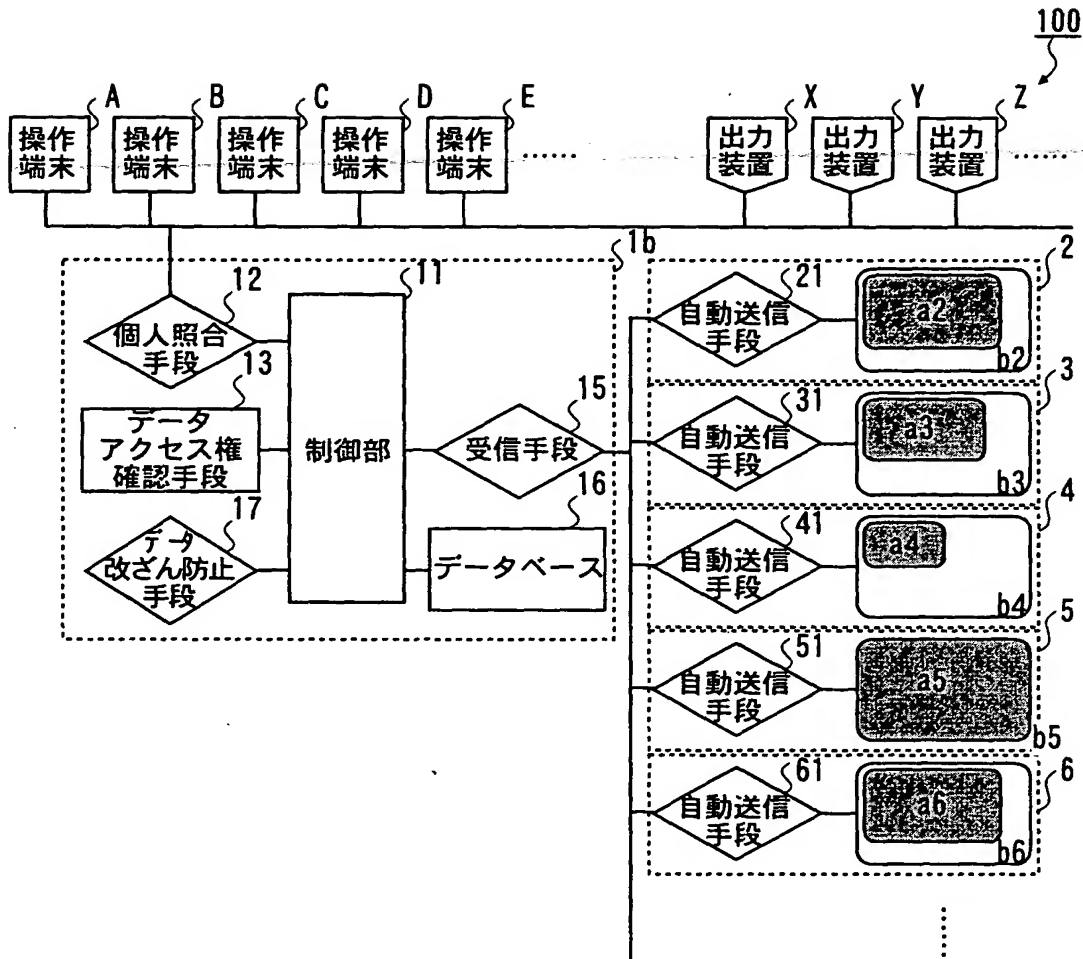
【図 4】



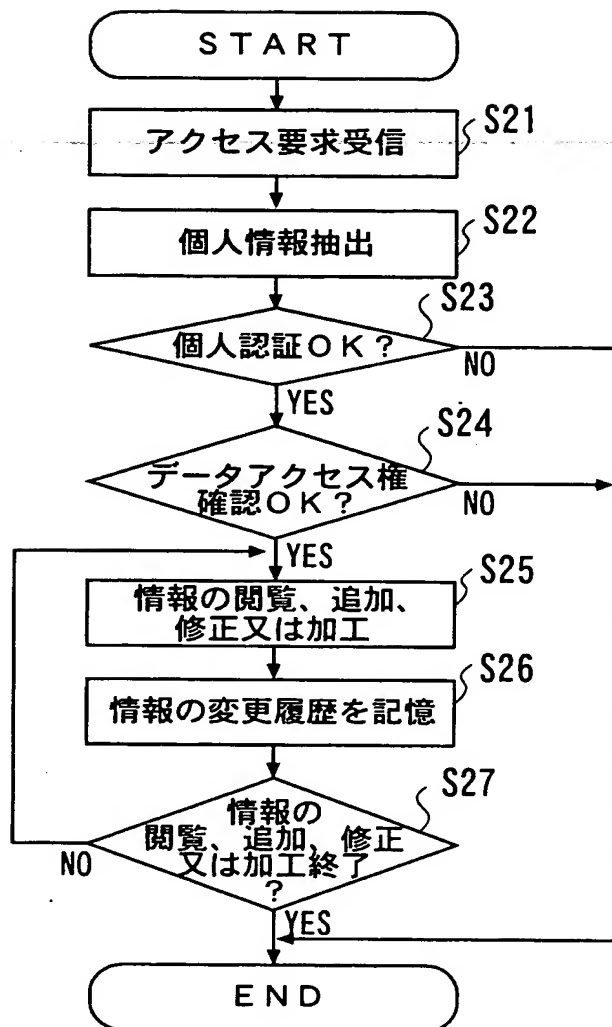
【図 5】



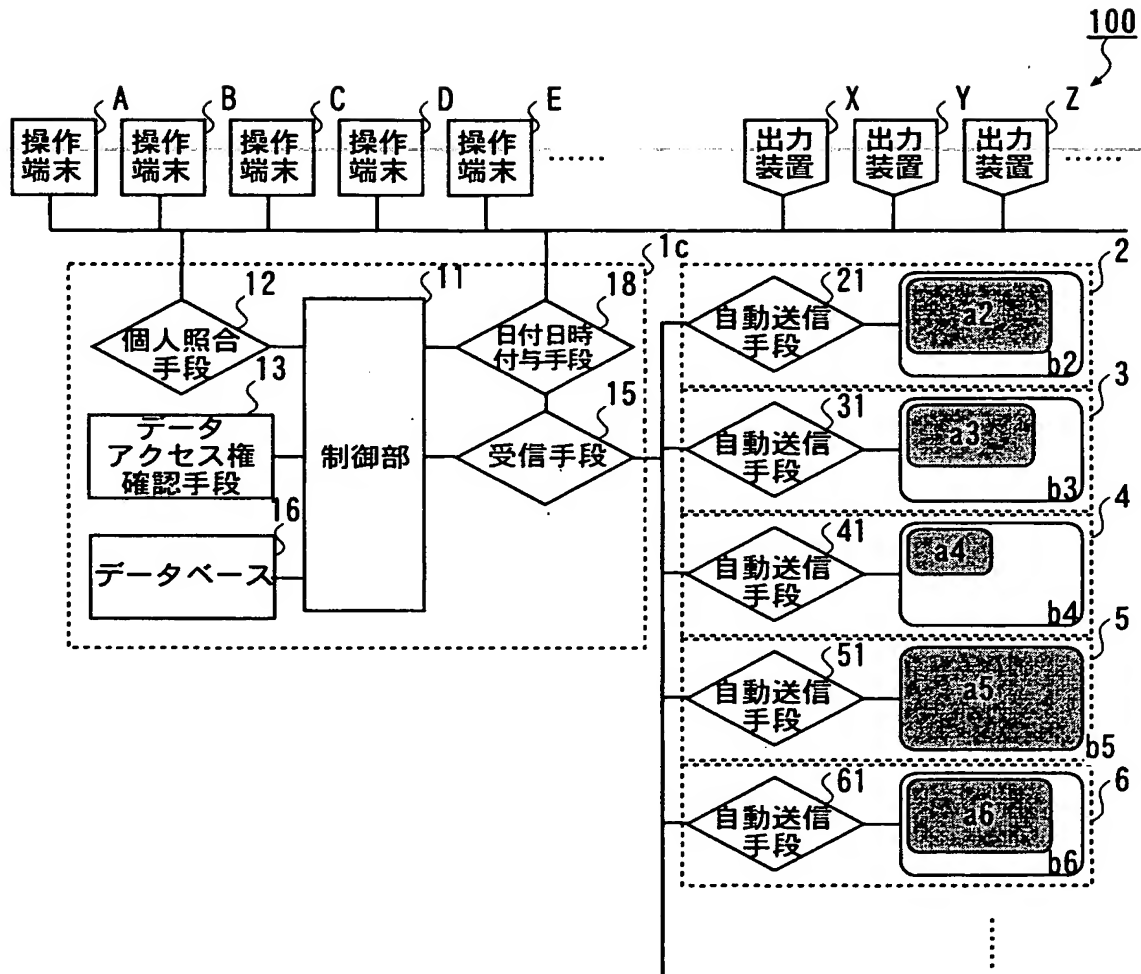
【図 6】



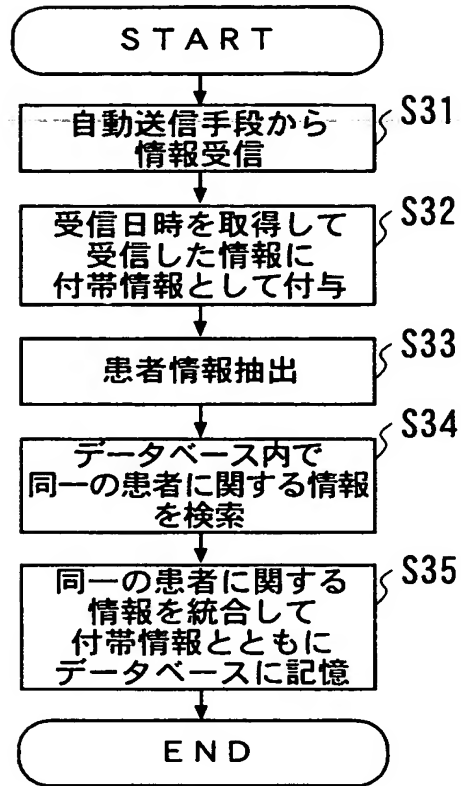
【図 7】



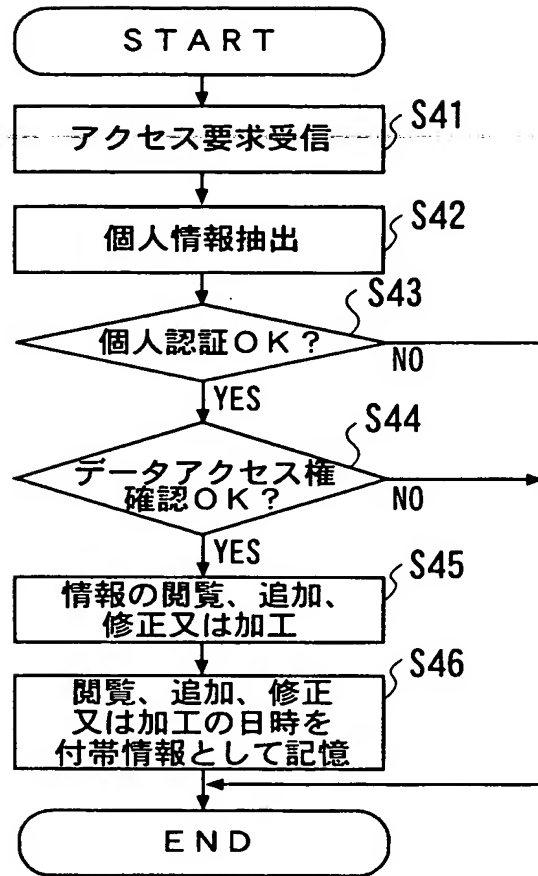
【図 8】



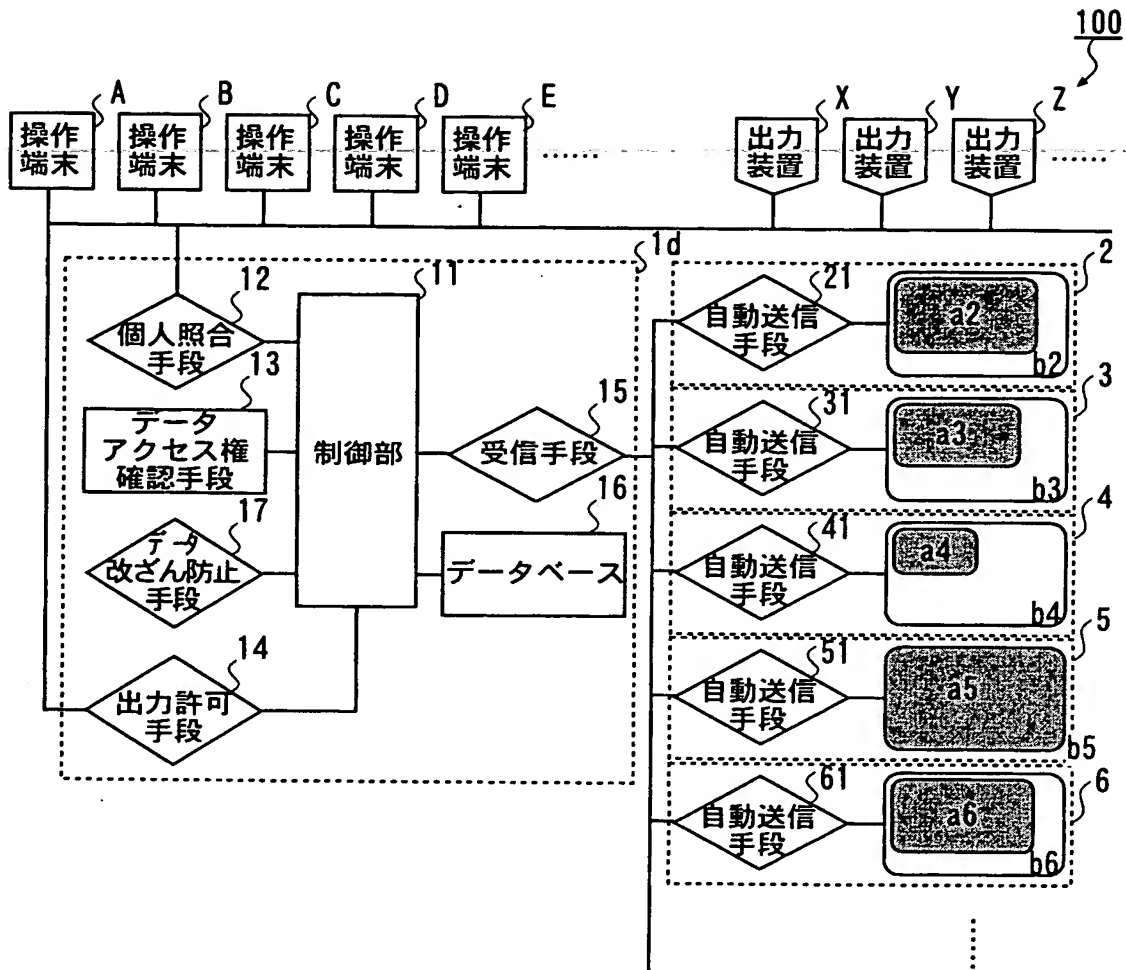
【図 9】



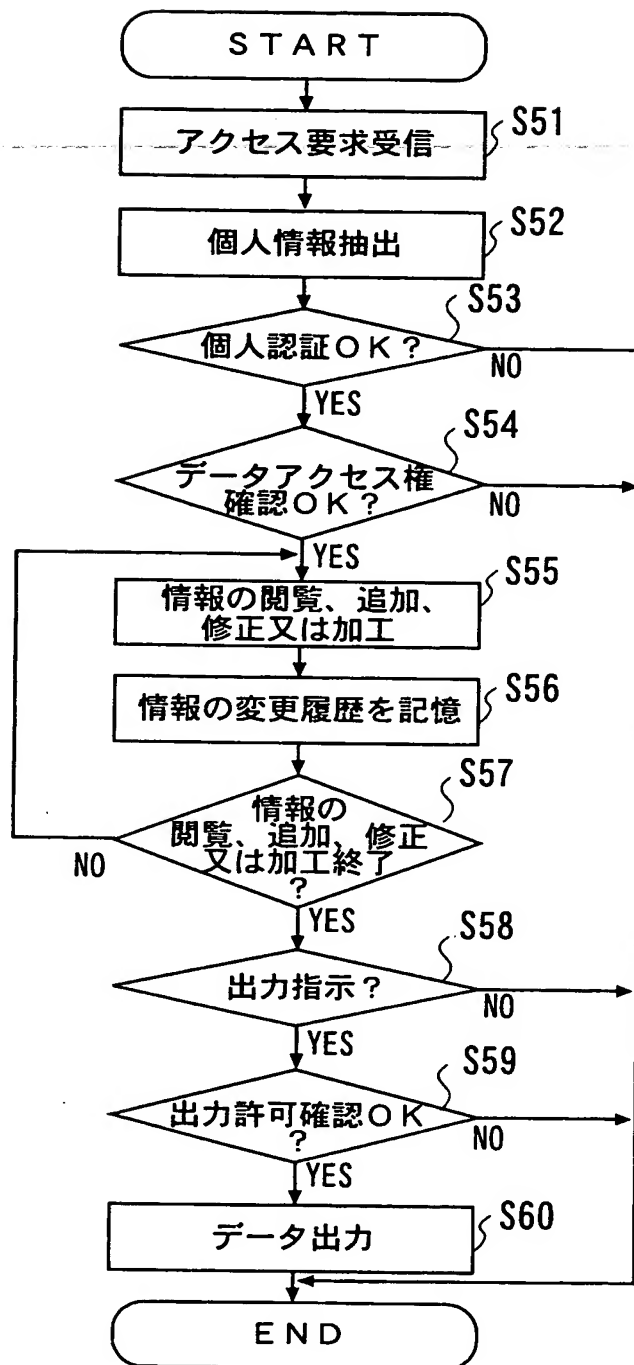
【図 1 0】



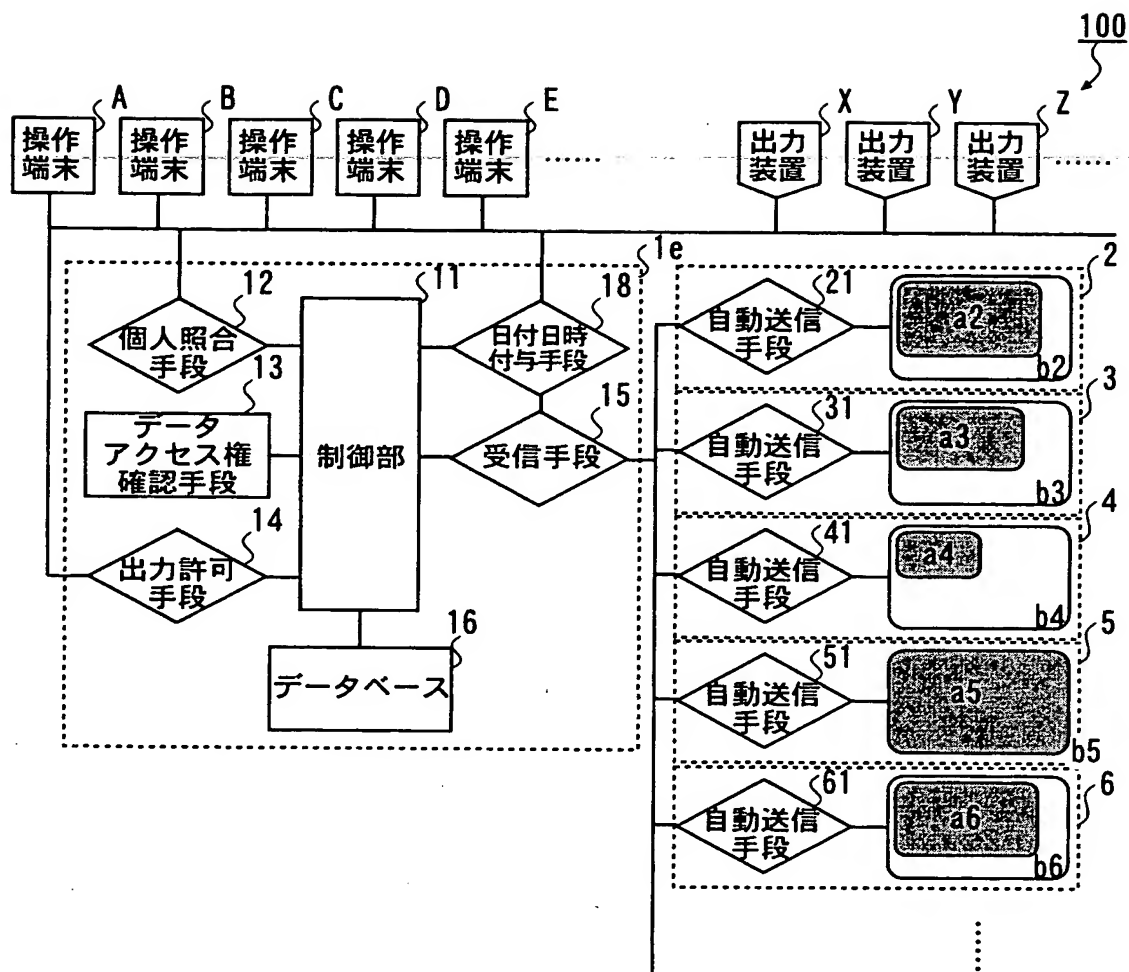
【図 1 1】



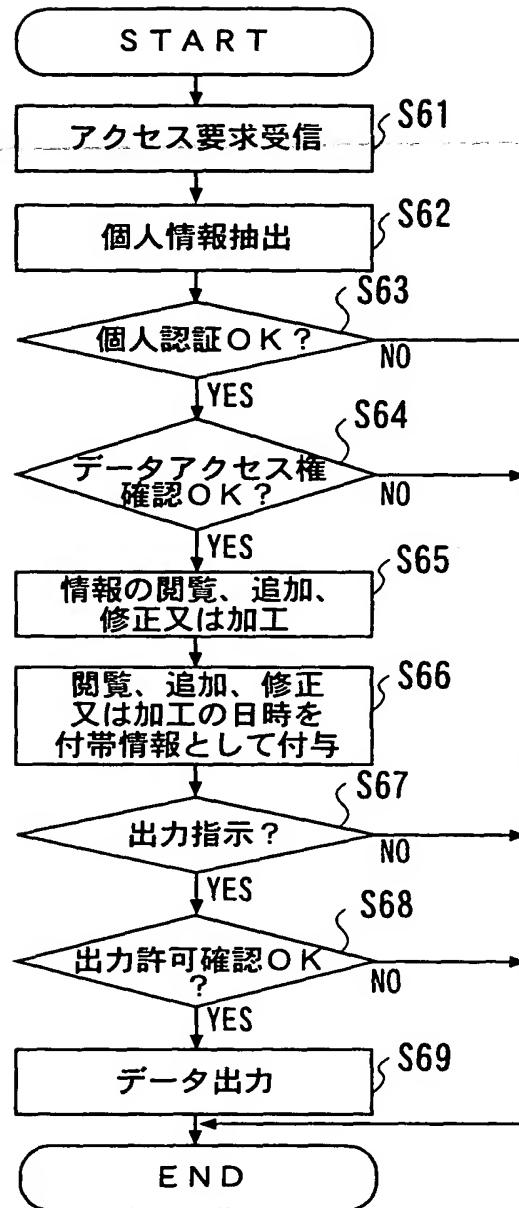
【図 1 2】



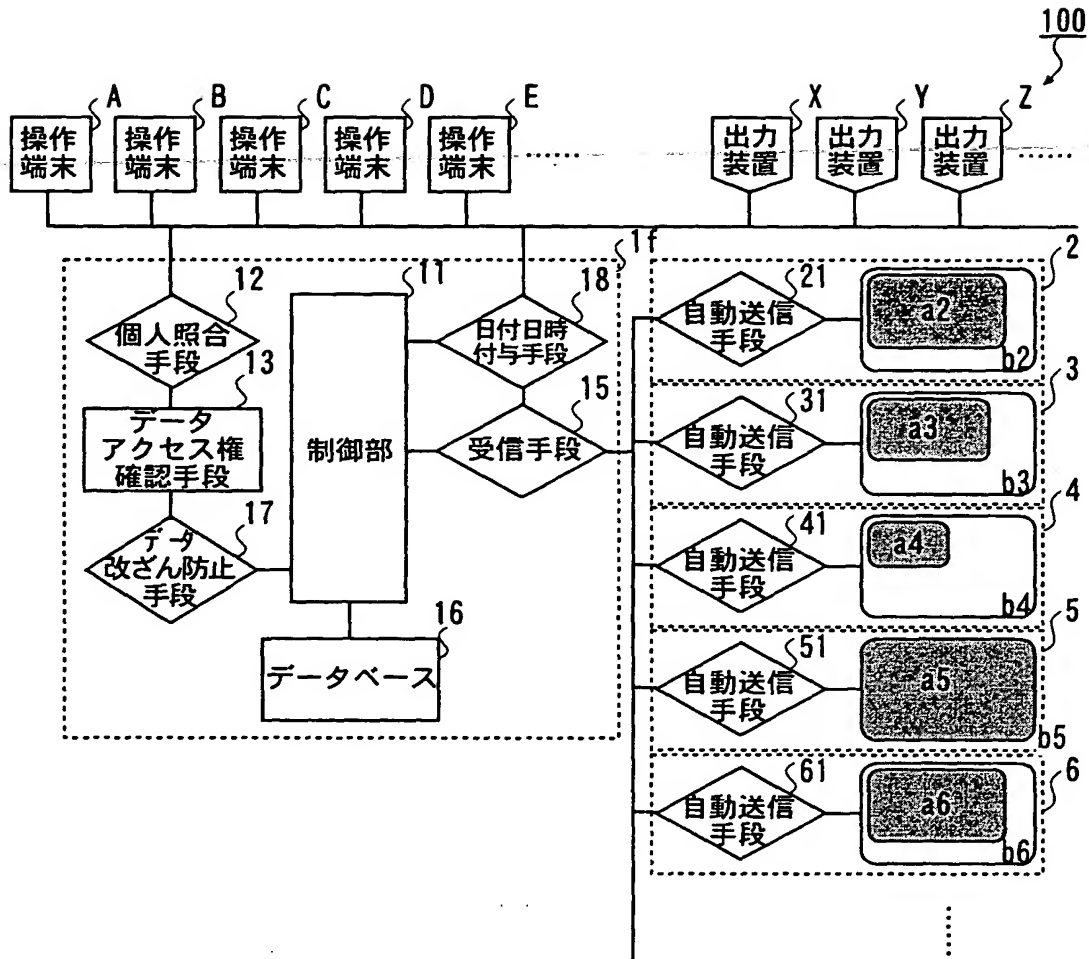
【図 13】



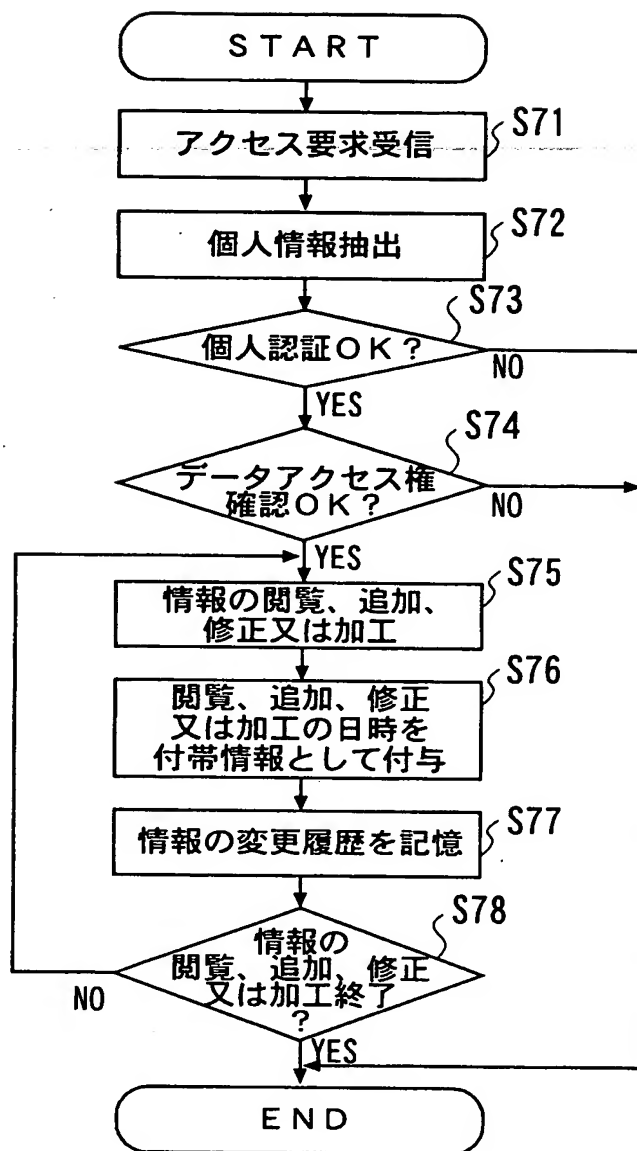
【図 1 4】



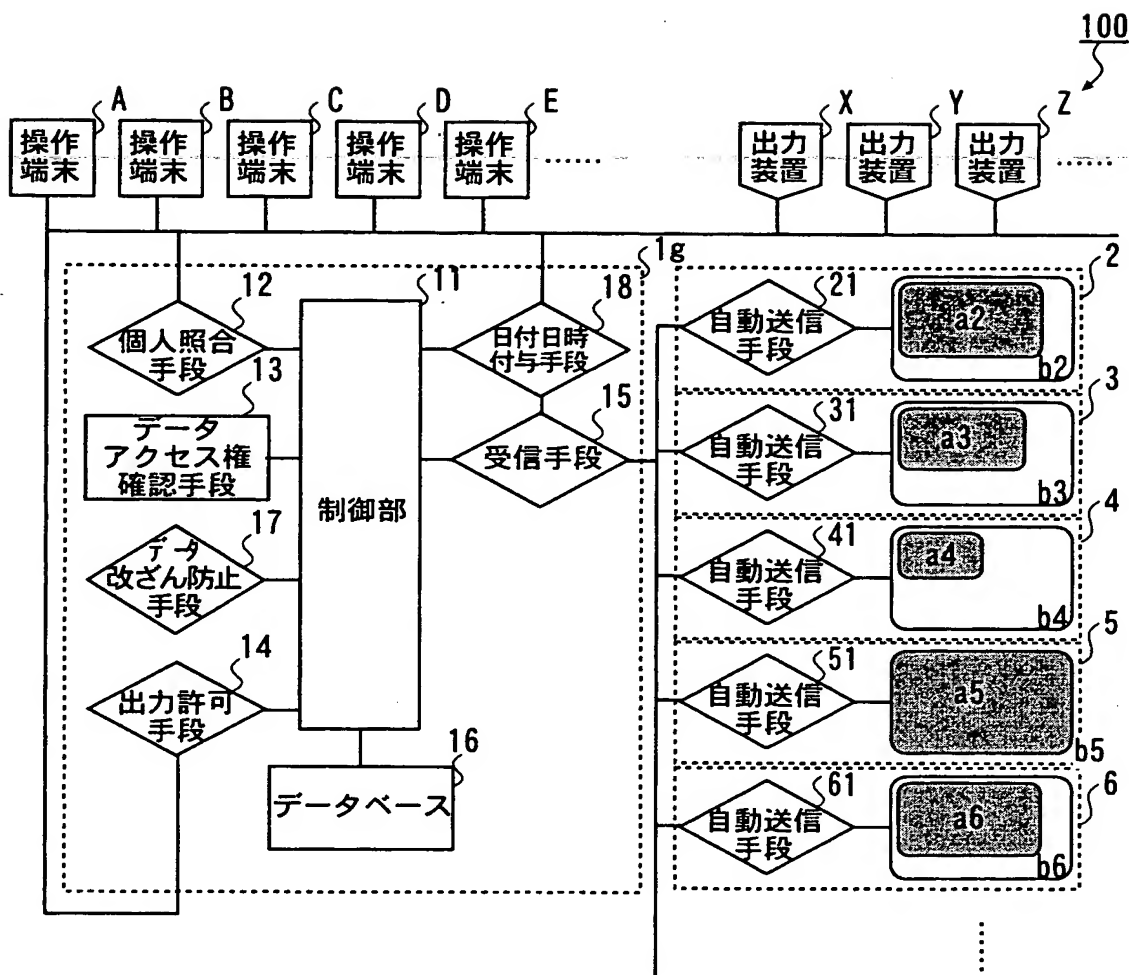
【図 15】



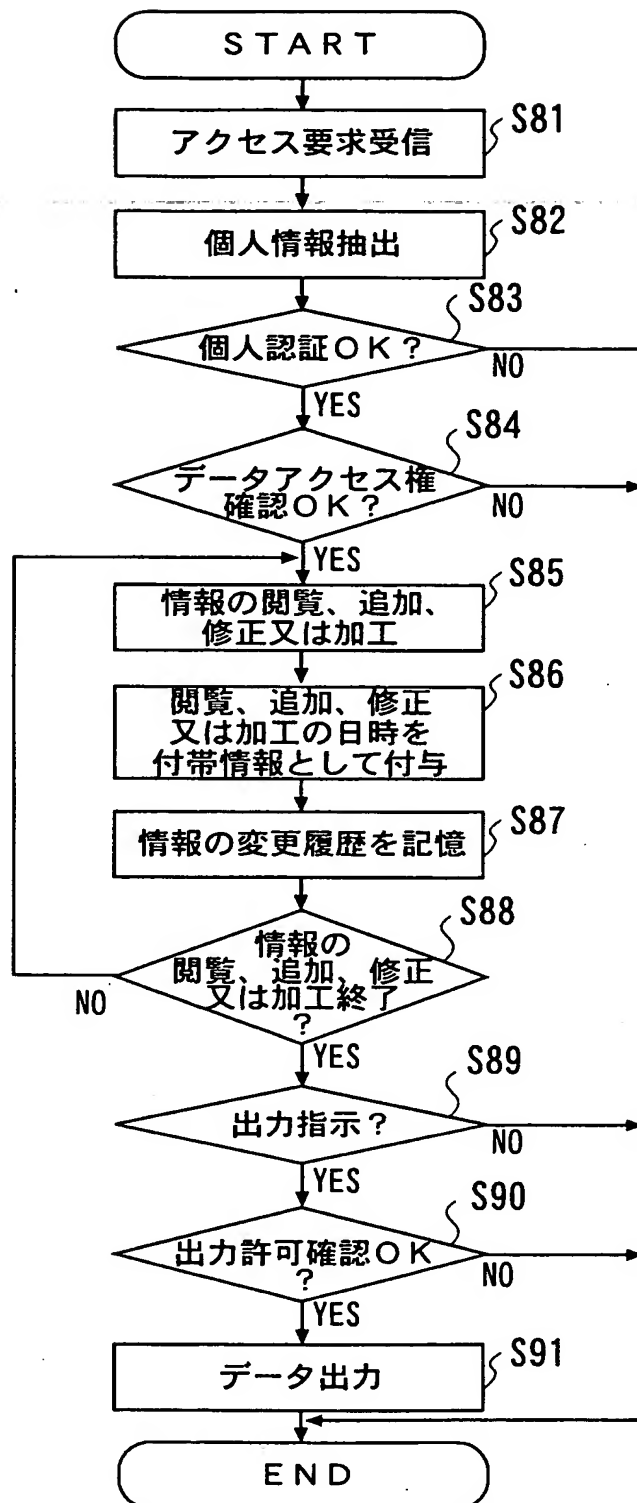
【図 1 6】



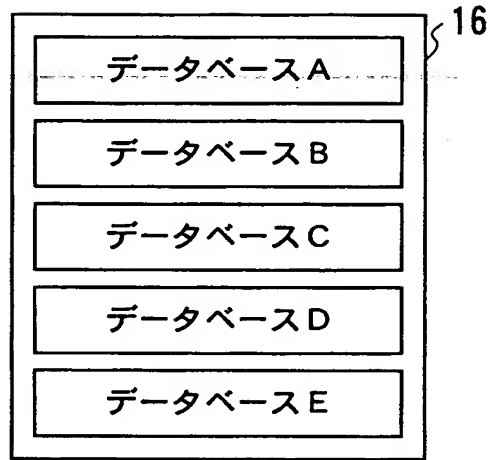
【図 17】



【図 1 8】



【図 1 9】



【書類名】 要約書

【要約】

【課題】 本発明の課題は、種々の医療情報が記憶されるデータベースに対するセキュリティを向上させることである。

【解決手段】 管理サーバ 1 a は、医療情報 DB 2 の自動送信手段 2 1 から送信される医療情報を、患者情報に基づいて患者毎に統合して管理し、この管理サーバ 1 a に蓄積された医療情報を利用するためには、個人照合手段 1 2 により、操作端末 A ～ E の操作者の個人認証を行い、この個人照合手段 1 2 により認証特定された操作者がアクセス可能な医療情報をデータアクセス権確認手段 1 3 により確認した上で、医療情報へのアクセスを許可する。

【選択図】 図 3

出 願 人 履 歴 情 報

識別番号

[000001270]

1. 変更年月日	1990年 8月14日
[変更理由]	新規登録
住 所	東京都新宿区西新宿1丁目26番2号
氏 名	コニカ株式会社